Administering Network Connectivity on Avaya Aura® Communication Manager

Release 6.3
555-233-504
Issue 19
June 2014

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Software" means Avaya's computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

- Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.
- Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than an Instance of the same database.
- CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.
- Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products", or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya and Avaya Aura® are trademarks of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Linux is the registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Software" means Avaya's computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

- Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Units may be linked to a specific, identified Server or an Instance of the Software.

- Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than an Instance of the same database.
- CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.
- Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products", or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

How to Get Help

For additional support telephone numbers, go to the Avaya support Website: http://www.avaya.com/support. If you are:

- Within the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the appropriate link for the type of support that you need.
- Outside the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the International Services link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

- IEC 60950-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.
- CAN/CSA-C22.2 No. 60950-1 / UL 60950-1 latest edition.

This product may contain Class 1 laser devices.

- Class 1 Laser Product
- Luokan 1 Laserlaite
- Klass 1 Laser Apparat

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards, as applicable:

- CISPR 22, including all national standards based on CISPR 22.
- CISPR 24, including all national standards based on CISPR 24.
- IEC 61000-3-2 and IEC 61000-3-3.

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

For a Class B digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Equipment With Direct Inward Dialing ("DID"):

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC's rules.

Proper Answer Supervision is when:

1. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
   - answered by the called station,
   - answered by the attendant,
   - routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
   - routed to a dial prompt
2. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

Permissible exceptions are:

- A call is unanswered
- A busy tone is received
- A reorder tone is received

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

Automatic Dialers:

When programming emergency numbers and (or) making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll Restriction and least Cost Routing Equipment:

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the

customer and the customer's employees from gaining access to the network and to these codes.

For equipment approved prior to July 23, 2001:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For equipment approved after July 23, 2001:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection:

Connection of this equipment to the telephone network is shown in the following table:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2.T	AS.2	RJ2GX, RJ21X, RJ11C
CO trunk	02GS2	0.3A	RJ21X, RJ11C
	02LS2	0.3A	RJ21X, RJ11C
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9.BN	6.0F	RJ48C, RJ48M
	04DU9.1KN	6.0F	RJ48C, RJ48M
	04DU9.1SN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9.DN	6.0Y	RJ48C

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242-2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. It is recommended that repairs be performed by Avaya certified technicians.

FCC Part 68 Supplier's Declarations of Conformity

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

Canadian Conformity Information

This Class A (or B) digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A (ou B) est conforme à la norme NMB-003 du Canada.

This product meets the applicable Industry Canada technical specifications/Le présent materiel est conforme aux specifications techniques applicables d'Industrie Canada.

European Union Declarations of Conformity

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Europeénne) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (2004/108/EC) and Low Voltage Directive (2006/95/EC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

European Union Battery Directive

Avaya Inc. supports European Union Battery Directive 2006/66/EC. Certain Avaya Inc. products contain lithium batteries. These batteries are not customer or field replaceable parts. Do not disassemble. Batteries may pose a hazard if mishandled.

Japan

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります。

If this is a Class A device:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス Ａ 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

If this is a Class B device:

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス Ｂ 情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 15
- Purpose 15
- Intended audience 15
- Document changes since last issue 15
- Related resources 16
  - Documentation 16
  - Training 17
  - Viewing Avaya Mentor videos 18
- Support 19
- Warranty 19

Chapter 2: Networking Overview 21
- Network terminology 21
- Digital telephone calls 21
- Network regions 22
  - Features affected by the increase in locations and network regions 25
- Inter-switch trunk connections 25
  - IP-connected networks 26
  - Branch office networks 26
  - Control networks 26
  - Spanning Tree Protocol 26
  - Inter-Gateway Alternate Routing 27
  - Dial Plan Transparency 28
- Network quality management 29
- VoIP-transmission hardware 29
  - Processor Ethernet 30
- LAN security 32
- Connection Preservation 33
  - Session refresh handling 33
  - Connection Preserving Migration 34

Chapter 3: Port network configurations 37
- IP port network connectivity 37
- Reliability 37
  - Simplex server 37
  - Duplex Server 38
- Simplex IP-PNC for the single control network 38
  - Architecture of simplex server IP-PNC 39
  - Duplicated TN2602AP circuit packs in IP-PNC PNs 41
  - Circuit packs for duplicated bearer connections 42
- Duplex IP-PNC (single control network) 42
  - Architecture of duplex IP-PNC single control network 43
- The Duplex server IP-PNC for a duplicated control network 46
  - Architecture of duplex IP-PNC duplicated control network 46
- The Duplex server IP-PNC for a duplicated control and bearer network connection 48
  - Architecture of duplex IP-PNC duplicated control and duplicated bearer network 49

Example of IP-PNC PNs with different reliability levels 51
Chapter 4: Control networks 55
Layer 2 connectivity options 55
Layer 3 connectivity options 57
Control network on customer LAN 59
Chapter 5: Converged Networks 63
Voice over IP converged networks 63
Network assessment 63
VoIP hardware 64
Universal DS1 circuit packs and MM710 T1/E1Media Module 65
TN799DP Control LAN 68
TN2302AP IP Media Processor 72
TN2602AP IP Media Resource 320 73
TN2312BP IP Server Interface (IPSI) 77
MM760 VoIP Media Module 81
Avaya gateways 83
IP trunks 83
SIP trunks 83
Creating a SIP trunk signaling group 84
H.323 trunks 85
Preparing to administer H.323 trunks 86
Verifying customer options for H.323 trunking 86
Administering C-LAN and IP Media Processor circuit packs (Simplex/Duplex Servers) 87
QoS parameters 88
IP node names and IP addresses 88
Assigning IP Node Names 88
Defining IP interfaces (C-LAN, TN2302AP, or TN2602AP Load Balanced) 89
Defining IP interfaces (duplicated TN2602AP) 90
Assigning link through Ethernet data module 90
Best Service Routing (optional) 91
Administering H.323 trunk 91
H323 trunk signaling group 92
Creating an H.323 trunk signaling group 92
Creating a trunk group for H.323 trunks 95
Modifying the H.323 trunk signaling group 96
Dynamic generation of private/public calling party numbers 97
Avaya Phones 98
IP Softphones 98
Avaya IP telephones 102
Hairpinning, shuffling, and Direct Media 106
Examples of shuffling 108
Hairpinning and shuffling administration interdependencies 115
Network Address Translation 117
Hairpinning and shuffling 120
Fax, modem, TTY, and H.323 clear-channel calls over IP trunks 126
Relay 127
Pass-through 127

T.38 ... 128
V.150.1 Modem Relay ... 128
Administering fax, TTY, modem, and clear-channel calls over IP trunks ... 129
FAX, TTY, modem, and clear channel transmission modes and speeds ... 129
Considerations for administering FAX, TTY, modem, and Clear-Channel transmission ... 134
Bandwidth for FAX, modem, TTY, and clear channel calls over IP networks ... 136
Media encryption for FAX, modem, TTY, and clear channel ... 137
SRTP media encryption ... 138
Platforms ... 139
Administering SRTP ... 139
Administering SRTP for video signaling ... 140
Chapter 6: Voice, Video, and Network quality administration ... 143
Factors causing voice degradation ... 143
Packet delay and loss ... 145
Echo ... 145
Transcoding ... 149
Bandwidth ... 149
Quality of Service (QoS) and voice quality administration ... 150
Layer 3 QoS ... 150
Layer 2 QoS: 802.1p/Q ... 151
IP CODEC sets ... 153
IP network regions ... 156
Call Admission Control ... 162
Administering DPT ... 166
Network Region Wizard ... 167
Manually interconnecting the network regions ... 168
Setting network performance thresholds ... 174
Enabling or disabling spanning tree ... 175
Jitter buffers ... 176
UDP ports ... 177
Media Encryption ... 177
Limitations of Media Encryption ... 177
Types of media encryption ... 178
License file ... 179
Legal wiretapping ... 183
Possible failure conditions ... 183
Interactions of Media Encryption with other features ... 183
Network recovery and survivability ... 184
Network management ... 184
H.248 link loss recovery ... 186
Administrable IPSI Socket Sanity Timeout ... 195
Survivable Core Servers ... 196
Improved Port Network Recovery from Control Network Outages ... 197
Port Network Recovery Rules screen ... 199
Survivability ... 200
Appendix A: PCN and PSN notifications ... 201
PCN and PSN notifications ... 201

Viewing PCNs and PSNs..... 201
Signing up for PCNs and PSNs..... 202
Index..... 203

Chapter 1: Introduction

Purpose

This book provides background information about the network components of Avaya Aura® Communication Manager.

You can refer to the book when you:

- Connect Avaya phones to various networks.
- Configure Avaya phones.
- Configure Port Networks (PN).
- Administer converged network components, such as gateways, trunks, fax, modem, TTY, and clear-channel calls.

Intended audience

This document is intended for anyone who wants to gain a high-level understanding of the product features, functionality, capacities, and limitations within the context of solutions and verified reference configurations.

- Technical support representatives
- Authorized Business Partners

Document changes since last issue

- Updated the topic Inter-Gateway Alternate Routing on page 27.
- Added a new topic Creating a SIP trunk signaling group on page 84.
- Modified the topic T.38 on page 128.

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Design		
Avaya Aura® Solution Design Considerations and Guidelines, 03-603978	Describes all the components that work with Communication Manager.	Solution Architects, Sales Engineers, Support Personnel
Implementation		
Avaya Aura® Communication Manager Survivable Options, 03-603633	Describes the survivable options. Also contains information about designing, configuring, administering, maintaining, and troubleshooting survivable options.	Implementation Engineers, Support Personnel
4600 Series IP Telephone Installation Guide, 555-233-128	Describes the equipment and resources required for installation, and how to set local administrative options.	Implementation Engineers, Support Personnel
Avaya one-X Deskphone Edition 9600 Series IP Telephone Installation and Maintenance Guide, 16-300694	Describes how to install and maintain the 9600 Series IP Telephone product line and troubleshoot telephone problems.	Implementation Engineers, Support Personnel
Avaya one-X Deskphone Value Edition 1600 Series IP Telephones Installation and Maintenance Guide, 16-601438	Describes the implementation of Communication Manager, DHCP, HTTP/HTTPS servers for 1600 Series IP Telephones, a Local Area Network (LAN), or a Web server.	Implementation Engineers, Support Personnel
Maintenance and Troubleshooting		
Maintenance Commands for Avaya Aura® Communication	Describes the commands for Communication Manager.	Solution Architects,

Title	Description	Audience
Manager, Branch Gateway and Servers, 03-300431		Implementation Engineers, Support Personnel
Administration		
Administering Avaya Aura® Communication Manager, 03-300509	Describes the procedures and screens for administering Communication Manager.	Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel
4600 Series IP Telephone LAN Administrator Guide, 555-233-507	Describes the administration of DHCP and TFTP servers to support the Avaya 4600 Series IP Telephones.	Implementation Engineers, Support Personnel
Avaya one-X Deskphone Edition 9600 Series IP Telephones Administrator Guide, 16-300698	Describes the administration of Communication Manager, DHCP, HTTP/HTTPS servers for 9600 Series IP Telephones, a Local Area Network (LAN), or a Web server.	Sales Engineers, Implementation Engineers, Support Personnel
Understanding		
Avaya Aura® Hardware Description and Reference, 555-245-207	Describes the hardware devices that can be incorporated in a Communication Manager telephony configuration.	Sales Engineers, Solution Architects, Support Personnel

Training

The following courses are available on https://www.avaya-learning.com. To search for the course, in the **Search** field, enter the course code and click **Go**.

Course code	Course title
Understanding	
1A00234E	Avaya Aura® Fundamental Technology
AVA00383WEN	Avaya Aura® Communication Manager Overview

Course code	Course title
ATI01672VEN, AVA00832WEN, AVA00832VEN	Avaya Aura® Communication Manager Fundamentals
Docu00158	Whats New in Avaya Aura® Release 6.2 Feature Pack 2
5U00060E	Knowledge Access: ACSS - Avaya Aura® Communication Manager and CM Messaging Embedded Support (6 months)
Implementation and Upgrading	
4U00030E	Avaya Aura® Communication Manager and CM Messaging Implementation
ATC00838VEN	Avaya Media Servers and Implementation Workshop Labs
4U00115V	Avaya Aura® Communication Manager Implementation Upgrade (R5.X to 6.X)
4U00115I, 4U00115V	Avaya Aura® Communication Manager Implementation Upgrade (R5.X to 6.X)
AVA00838H00	Avaya Media Servers and Media Gateways Implementation Workshop
ATC00838VEN	Avaya Media Servers and Gateways Implementation Workshop Labs
Administration	
AVA00279WEN	Communication Manager - Configuring Basic Features
AVA00836H00	Communication Manager Basic Administration
AVA00835WEN	Avaya Communication Manager Trunk and Routing Administration
5U0041I	Avaya Aura® Communication Manager Administration
AVA00833WEN	Avaya Communication Manager - Call Permissions
AVA00834WEN	Avaya Communication Manager - System Features and Administration
5U00051E	Knowledge Access: Avaya Aura® Communication Manager Administration

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support web site, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support web site, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com under **Help & Policies> Policies & Legal > Warranty and Product Lifecycle**. See also **Help & Policies > Policies & Legal > License Terms**.

Chapter 2: Networking Overview

Network terminology

The Communication Manager network can contain multiple servers and equipment, including data-networking devices that servers control. Such equipment might be geographically dispersed across many sites. Each site might segregate equipment into distinct logical groupings of endpoints, including stations, trunks, and gateways, referred to as network regions. A single server system has one or more network regions. If one server is inadequate for controlling the equipment, multiple systems can be networked together. One or more network regions make a site, and one or more sites make a system, which in turn is a component of a network.

The following provides a better understanding of network terminology:

- Businesses have a corporate network, such as a LAN or a WAN. Over this corporate network businesses distribute emails and data files, run applications, gain access to the Internet, and exchange fax and modem calls.

  This type of network and the traffic that it bears is a nondedicated network. The network is a heterogeneous mix of data types.
- A non dedicated network that carries digitized voice signals with other data types is a converged network. The converged network is a confluence of voice and nonvoice data.
- Network segments that carry telephony traffic are dedicated networks because the network segments carry only telephony-related information.
- A digital network carries telephony and nontelephony data in a packet-switched environment, such as TCP/IP, instead of a circuit-switched environment, such as TDM. The digital network is an IP network.

Digital telephone calls

A digital telephone call consists of voice data and call-signaling messages. Some transmission protocols require transmission of signaling data over a separate network, virtual path, or channel from the voice data. The following list describes the data that is transmitted between switches during a telephone call:

- Voice data: Digitized voice signals
- Call-signaling data: Control messages
- Distributed Communications System (DCS) signaling data:

  Use DCS to configure two or more communication switches as a single switch. DCS provides attendant and voice-terminal features between these switch locations. DCS simplifies dialing procedures and ensures transparent use of some of the Communication Manager features. Feature transparency means that features are available to all users on DCS regardless of the switch location.

Network regions

A network region is a group of IP endpoints that share common characteristics and common resources. Every IP endpoint on the Communication Manager system belongs to a network region. You can differentiate between the network regions either by the resources assigned or the geographical location or both.

The following are the common reasons to create different network regions when a group of endpoints:

- Require a different codec set based on bandwidth allocation or a different encryption algorithm than another group.
- Gain access to specific C-LANs, MedPros, gateways, or other resources.
- Require a different UDP port range or QoS parameters than another group.
- Report to a different VoIP Monitoring Manager server than another group.
- Require a different codec set based on bandwidth requirement or encryption algorithm for calls within the group than calls between separate endpoint groups.

The concept of locations is also similar to network regions. Use the location parameter to:

- Identify distinct geographic locations, primarily for call routing purposes.
- Ensure that calls pass through proper trunks based on the origin and destination of each call.

Communication Manager supports 2000 locations and network regions. This increase in the number of network regions and locations applies to customers that use Communication Manager installed on the following servers:

- S8800
- S8510
- HP ProLiant DL360 G7
- HP ProLiant DL360p G8

- Dell™ PowerEdge™ R610
- Dell™ PowerEdge™ R620

With the increase in the number of network regions and locations that Communication Manager supports, organizations can expand businesses to various locations globally. Organizations can also efficiently manage bandwidth by allocating the required bandwidth between a pair of network regions.

To support the increase to 2000 network regions and locations, you can now configure network regions as core network regions and stub network regions. You can configure network regions from 1 to 250 as core network regions or stub network regions. Network regions 251 to 2000 are stub network regions.

A core network region is the traditional network region and can have multiple direct links with other network regions. For a diagrammatic representation of core network regions, see Core network regions on page 23. The solid lines in the diagram indicate a direct communication path between two core network regions. The dotted lines indicate an indirect logical communication path between two core network regions.

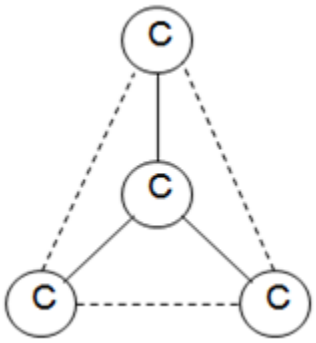


Figure 1: Core network regions

A stub network region must have a single defined pathway to only one core network region. For a diagrammatic representation of core network regions and stub network regions, see Core and stub network regions on page 24.

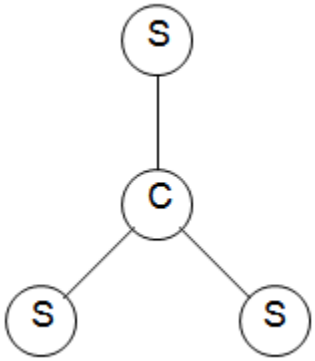


Figure 2: Core and stub network regions

Stub network regions communicate with other network regions using the defined communication pathways of the core network regions. For example, if stub network region 251 directly communicates with core network region 1, and stub network region 251 wants to send data to core network region 3, then stub network region 251 first sends data to core network region 1. From core network region 1, Communication Manager uses the predefined communication pathway of core network region 1 to reach core network region 3. For a diagrammatic representation of the communication pathway, see Communication Pathway from a stub network region to a core network region on page 24.

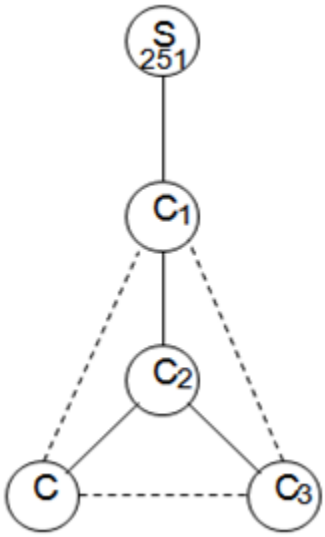


Figure 3: Communication Pathway from a stub network region to a core network region

The benefit of having a stub network region is that you do not have to configure multiple communication pathways to different network regions. With the introduction of stub networks, when you add a stub network region, you must administer the communication path only to the core network region that the stub network region connects to.

You must assign all Communication Manager hardware, such as branch gateways, media processors, C-LANs, and G650 cabinets to network regions 1 to 250 regardless of whether the network region is a core network region or a stub network region.

Features affected by the increase in locations and network regions

The increase in the number of network regions and locations can affect the following features:

- Dial Plan Transparency (DPT): The DPT feature can work in an endpoint-only stub network region. Stub network regions use the media processing resources of the core network regions that the stub network regions connect to. If you administer the DPT feature in a core network region that is directly linked with other stub network regions, then during a network outage, the endpoints in the stub network regions can connect to endpoints in other network regions.
- Inter-gateway Alternate Routing (IGAR): Any stub network region from 1 to 250 can use IGAR if the stub network region contains a branch gateway or a port network. IGAR is unavailable for stub network regions from 251 to 2000.
- Emergency Calling: When an endpoint in a stub network region dials an emergency number, Communication Manager analyzes the dialed number and uses the ARS location table to route the call to the destination. The call is routed using a predefined route pattern.

Inter-switch trunk connections

You can use the connected switches within an enterprise to communicate easily, regardless of the location or the communication server that the switches use. Inter-switch connections also provide shared communications resources, such as messaging and call center services.

Switches communicate with each other over trunk connections. There are many types of trunks that provide different sets of services. Commonly used trunk types are:

- Central Office (CO) trunks that provide connections to the public telephone network through a central office.
- H.323 trunks that send voice and fax data over the Internet to other systems with H.323 trunk capability.
- H.323 trunks that support DCS+ and QSIG signaling.
- Tie trunks that connect switches in a private network.

For more information about the trunk types, see *Administering Avaya Aura® Communication Manager*, 03-300509.

IP-connected networks

For detailed examples of IP-connected (IP-PNC) networks, see Chapter 3: Port network configurations on page 37.

Branch office networks

For Communication Manager environments, the MultiVOIP™ gateways provide distributed networking capabilities to small branch offices of large corporations. MultiVOIP extends the call features of a centralized Avaya server. MultiVOIP provides local office survivability to branch offices of up to 15 users who use analog or IP telephones.

For more information about MultiVOIP™ gateways, go to http://www.multitech.com/PARTNERS/Alliances/Avaya/.

Control networks

Control networks are networks over which Communication Manager exchanges signaling data with the port networks. Communication Manager exchanges signaling data through the IPSI circuit packs.

Spanning Tree Protocol

Spanning Tree Protocol (STP) is a loop avoidance protocol. If you do not have loops in your network, you do not need STP. However, you must always enable STP. If you do not enable STP on a network that has a loop, or which has wrong cable plugged into wrong ports, all the traffic stops.

However, STP is slow to converge after a network failure and provide a new port into the network. By default the speed is ~50 seconds.

A modified version of STP is the Rapid Spanning Tree protocol. Rapid Spanning Tree converges faster than STP and enables new ports faster than the older protocol. As the Rapid Spanning Tree protocol works with all Avaya equipment, use the Rapid Spanning Tree protocol.

Inter-Gateway Alternate Routing

With the Inter-Gateway Alternate Routing (IGAR), Communication Manager can use the PSTN when the IP-WAN cannot carry the bearer connection for the single-server systems that use the IP-WAN to connect bearer traffic between port networks or gateways.

Note:

Communication Manager Release 6.3.5 and earlier supported IGAR for analog, DCP, and H.323 endpoints. Communication Manager Release 6.3.6 extends this support to SIP endpoints.

IGAR requests PSTN to provide bearer connections in any of the following conditions:

- The number of calls allocated or bandwidth allocated through Call Admission Control-Bandwidth Limits (CAC-BL) is reached.
- VoIP RTP resource exhaustion in a port network or media gateway is encountered.
- The codec set between a pair of network regions is set to `pstn`.
- Forced redirection is configured between a pair of network regions.

IGAR provides enhanced Quality of Service (QoS) to large distributed single-server configurations. IGAR is intended for configurations where the IP network is not reliable enough to carry bearer traffic. If you have more than one IP network available, you can use H.323 or SIP trunks for IGAR instead of the PSTN.

When Communication Manager needs an inter gateway connection and adequate IP bandwidth is unavailable, Communication Manager attempts to substitute a trunk connection for the IP connection. For example, Communication Manager can substitute a trunk connection in any of the following situations:

- A user in one Network Region (NR) calls a user in another NR
- A station in one NR bridges on to a call appearance of a station in another NR
- An incoming trunk in one NR routes to a hunt group with agents in another NR
- An announcement or music source from one NR must be played to a party in another NR

Communication Manager attempts to use a trunk for inter-region voice bearer connection when the following five conditions are met:

- An inter gateway connection is needed.
- IGAR requests PSTN to provide bearer connections.
- IGAR is enabled for the NRs associated with each end of the call.

- The **Enable Inter-Gateway Alternate Routing** system parameter is set to `y`.
- The number of trunks used by IGAR in each NR is not reached the limit administered for that NR.

The SRC PORT TO DEST PORT TALKPATH page of the status station screen shows the IGAR trunk connectivity for an interNR call.

A Trunk Inter-Gateway Connection (IGC) is established using ARS to route a trunk call from one NR to IGAR Listed Directory Number (LDN) extension administered for other NR. The Trunk IGC is independent of the call. Therefore, Communication Manager can originate the IGC from the NR of the calling party to the NR of the called party, or vice versa. However, for users who use Facility Restriction Levels or Toll Restriction to determine who gets access to IGAR resources during a WAN outage, the calling user is considered the originator of the Trunk IGC for authorization and routing. However, if the outgoing trunk group is administered to send the Calling Number, the IGAR Extension in the originating NR is used to create this number using the appropriate administration.

The following are examples of failure scenarios and how Communication Manager handles the scenarios:

- On a direct call, the call continues to the first coverage point of the unreachable called endpoint, or if no coverage path is assigned, busy tone is played to the calling party.
- If the unreachable endpoint is accessed through a coverage path, the coverage point is skipped.
- If the unreachable endpoint is the next available agent in a hunt group, that agent is considered unavailable, and the system tries to route the call to another agent using the administered group type, such as Circular distribution and Percent Allocation Distribution.

Dial Plan Transparency

Dial Plan Transparency (DPT) preserves the dial plan when a gateway registers with a Survivable Remote server or when a port network registers with a Survivable Core server. This is due to the loss of contact with the primary controller. DPT establishes a trunk call and reroutes the call over the PSTN to connect endpoints that can no longer connect over the corporate IP network.

DPT does not need to be activated in the license file. DPT is available as a standard feature for Communication Manager Release 4.0 and later. DPT is similar to IGAR as both provide alternate call routing when normal connections are unavailable. A major difference is that DPT routes calls between endpoints controlled by two independent servers. IGAR routes calls between endpoints controlled by a single server. The DPT and IGAR features are independent of each other, but you can activate both simultaneously.

Limitations of DPT:

- DPT only handles IP network connectivity failures between network regions.
- DPT calls are trunk calls. Therefore, Communication Manager does not support many station features.
- For Release 4.0, DPT applies only to endpoints that are dialed directly. DPT cannot route redirected calls or calls to groups.
- DPT cannot reroute calls involving a SIP endpoint that has lost registration with the Home SES.
- DPT works only when failover strategies for gateways and port networks, and alternate gatekeeper lists for IP stations are consistent.

For information about administering DPT, see Administering DPT on page 166.

Network quality management

A successful Voice over Internet Protocol (VoIP) implementation involves quality of service (QoS) management that is affected by three major factors:

- Delay: Significant end-to-end delay can cause echo and talker overlap.
- Packet Loss: Under peak network loads and periods of congestion, voice data packets can be dropped.
- Jitter (Delay Variability): Jitter results when data packets arrive at their destination at irregular intervals because of variable transmission delay over the network.

For more information about these QOS factors and network quality management, see:

- Chapter 6: Voice and Network quality administration on page 143.
- *Avaya Aura® Solution Design Considerations and Guidelines*, 03-603978.

VoIP-transmission hardware

The following circuit packs are essential in an Avaya telecommunications network:

- TN799DP control LAN (C-LAN) interface

  Provides TCP/IP connectivity over Ethernet between servers and gateways, or Point to Point Protocol (PPP) between servers and adjuncts.

- TN2312BP IP Server Interface (IPSI)

  Transports control messages between servers and port networks.

- TN2302AP IP Media Processor and TN2602AP IP Media Resource 320

Provides high-capacity VoIP audio access to the switch for local stations and outside trunks.

- Branch gateways

  Provides:

  - Extension of Communication Manager telephony features to branch offices when controlled by a remote server.
  - Standalone telephony systems when controlled by an embedded S8300D server.
  - Survivable Remote server backup for a remote server.

  The branch gateways include the G700, G250, G350, G430, G450, and IG550.

- MM760 VoIP Media Module

  Provides another 64 VoIP channels in the G700 motherboard VoIP engine. The MM760 VoIP Media Module is a clone of the G700.

For more information about Avaya hardware devices, see *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

For information about the administration tasks for this equipment, see VoIP hardware on page 64.

Processor Ethernet

Processor Ethernet (PE) provides connectivity to IP endpoints, gateways, and adjuncts. The PE interface is a logical connection in the Communication Manager software that uses a port on the NIC in the server. The NIC is the s-called native NIC. PE uses the PROCR IP-interface type. You do not need additional hardware to implement PE.

During the configuration of a server, PE is assigned to a Computer Ethernet (CE). PE and CE share the same IP address, but are different in nature. The CE interface is a native computer interface while the PE interface is the logical appearance of the CE interface within Communication Manager software. The interface that is assigned to PE can be a control network or a corporate LAN. The interface that is selected determines which physical port PE uses on the server.

For more information about how to configure the server, see *Administering Avaya Aura® Communication Manager*, 03-300509.

A Survivable Remote server or a Survivable Core server enables the Processor Ethernet interface automatically. Using the PE interface you can register H.248 gateways and H.323 endpoints on the Survivable Remote server. You must set the H.248 and the H.323 fields on the IP Interface Procr screen to the default value `yes`.

In Communication Manager release 5.2 and later, Branch Gateway and H.323 endpoint registration on the Survivable Core server is possible. You must administer the **Enable PE for H.248 Gateways** and the **Enable PE for H.323 Endpoints** fields on the Survivable

Processor screen of the main server. The IP Interface Procr screen of the Survivable Core server displays the values that you administered for the H.248 and H.323 fields.

Important:

Both the Survivable Core server and the Survivable Remote server require the PE interface to register to the main server. Do not disable the PE interface on either of the servers.

Support for Processor Ethernet and port networks on a Survivable Core server

In Communication Manager Release 5.2 and later, the capabilities of Survivable Core servers are enhanced to support the connection of IP devices to the Processor Ethernet (PE) interface and to C-LAN interfaces. C-LAN interfaces are located in G650 gateways. G650 are port networks.

A Survivable Core server can use the PE interface to support IP devices, such as Branch Gateway, H.323 Gateways, IP Adjuncts, IP telephones, IP trunks, and SIP trunks. The Survivable Core server can optionally control port networks through IPSI simultaneously. When there are no port networks in the configuration, the Survivable Core server can provide the equivalent benefit of an Survivable Remote server. The Survivable Core server can be duplicated, providing more redundancy to the survivability of the system.

For PE on duplex servers to work, you must assign the PE interface to the PE Active server IP address and not the server unique address. The NIC assigned to the Processor Ethernet interface must be on a LAN connected to the main server.

- If the Survivable Remote server or the Survivable Core server registers to the C-LAN on the main server, the C-LAN must have IP connectivity to the LAN. The LAN must be assigned to the NIC used for PE on the Survivable Core server.
- If the Survivable Remote server or the Survivable Core server registers to PE on the main server, PE must have IP connectivity to the LAN. The LAN must be assigned to the NIC used for PE on the Survivable Core server.

Firmware for optimal performance

Processor Ethernet on duplex servers works effectively only when the branch gateways and IP telephones are on the current release of the firmware.

Use the following IP telephone models to ensure optimal system performance when you use Processor Ethernet on duplex servers:

- 9610, 9620, 9630, 9640, and 9650 telephones with firmware 3.0 or later. Any later 96xx and 96x1 models that support Time to Service (TTS) work optimally.
- 4601+, 4602SW+, 4610SW, 4620SW, 4621SW, 4622SW, and 4625SW Broadcom telephones with firmware R 2.9 SP1 or later. 46xx telephones are supported if the 46xx telephones are not in the same subnet as the servers.

All other IP telephone models must re-register if there is a server interchange. The 46xx telephones re-register if the telephones are in the same subnet as the servers.

To ensure that you have the most current versions of firmware, go to the Avaya Support website at http://support.avaya.com. Click **Downloads** and select the product.

LAN security

Customers do not want users to gain access to the switch using the INADS line, to C-LAN, and then gain access to a customer LAN. The Avaya architecture prevents users to gain access to the customer LAN. Figure Security-related system architecture shows a high-level switch schematic with a TN799 (C-LAN) circuit pack.

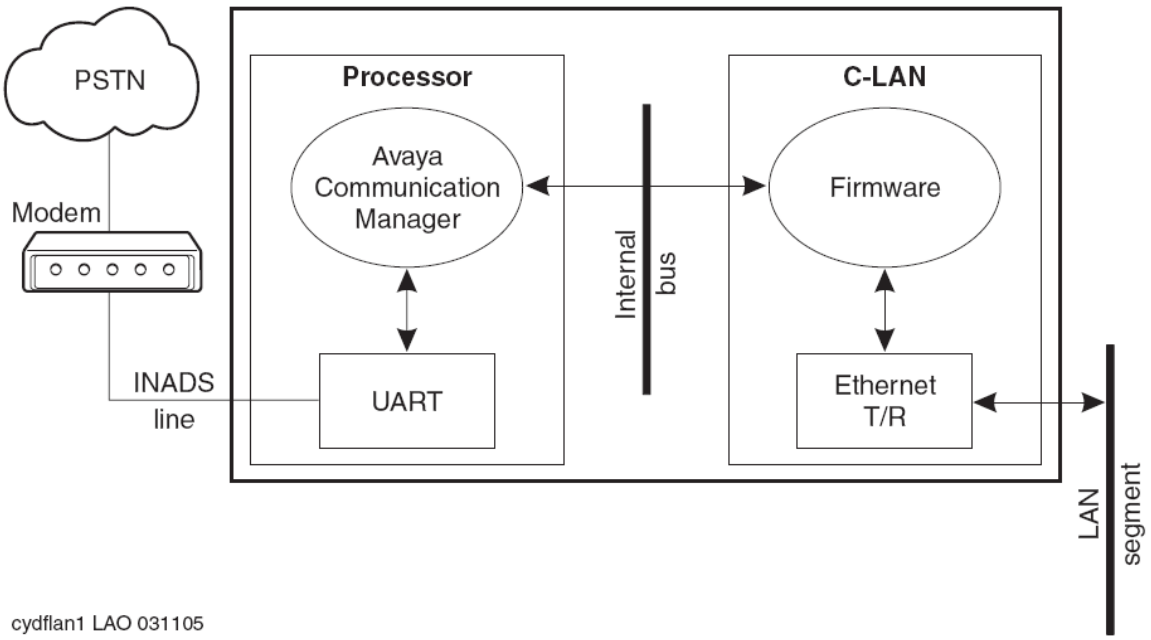


Figure 4: Security-related system architecture

Logins through the INADS line end in software. Software communicates with firmware over an internal bus through a limited message set. Two main reasons why a user cannot access the customer LAN through the INADS line are:

- A user logging into software cannot get direct access to the C-LAN firmware.

  The user can only enter SAT commands that request C-LAN information or to configure C-LAN connections.

- Communication Manager disables the C-LAN application TFTP and cannot enable the application.

  TELNET only interconnects C-LAN Ethernet clients to the system management application on the switch. FTP exists only as a server and is used only for firmware downloads. FTP cannot connect to the client network.

Connection Preservation

Communication Manager supports Connection Preservation and Call Preservation for handling SIP calls. Any SIP telephone connected to Communication Manager through a SIP enablement server can use this feature. SIP Connection Preservation and Call Preservation are always active.

Call Preservation and Connection Preservation during LAN failure

When the near-end failure is detected, the SIP signaling group state changes to the Out-of-service state. The SIP-trunk in the trunk group is in a deactivated state and cannot be used either for incoming or outgoing calls. Stable or active calls on the SIP-trunk are not dropped and are kept in the In-service/active state. When the active connection is dropped, SIP-trunk changes to the Out-of-service state. When the far-end failure is detected, the SIP signaling group is put into the Far-end-bypass state. Stable or active calls are not dropped and the SIP-trunk changes to the pending-busyout state. When the active connection is dropped, SIP-trunk changes into the Out-Of-Serivce/FarEnd-idle state.

Call Preservation and Connection Preservation when LAN connectivity is revived

When the near-end failure ends, the SIP signaling group state changes to the In-service/active state. Stable or active calls on the SIP-trunk are kept in the In-service/active state. When the far-end failure ends, the SIP signaling group state changes to the In-service/active state. State of Stable or active calls on the SIP-trunk changes from pending-busyout to the In-service/active state.

The Connection Preservation mechanism works with DCP and H.323 telephones also.

Session refresh handling

When SIP session refresh handling fails, the SIP call is set to Connection Preservation and a net safety timer keeps the call active for 2 hours. After 2 hours the call drops, unless the user ends the call before time.

Connection Preserving Migration

The Connection Preserving Migration (CPM) feature preserves bearer connections while Branch Gateway migrates from one Communication Manager server to another because of network or server failure. Users on connection preserved calls cannot use features, such as Hold, Conference, or Transfer. In addition to preserving the audio voice paths, CPM extends the period for recovery operations and functions during the complementary recovery strategies of Avaya.

H.248 and H.323 link recovery

The H.248 link is a link between a Communication Manager server and a gateway. The H.323 link is a link between a gateway and an H.323-compliant IP endpoint. The link recovery is an automated method in which the gateway reacquires the link after the link is lost from either a primary call controller or a Survivable Remote server. The H.248 link and the H.323 link provide the signaling protocol for:

- Call setup
- Call control while the call is in progress
- Call tear-down

If the link goes out of service, the link recovery preserves calls and attempts to reestablish the original link. If the gateway or the endpoint cannot reconnect to the original server or gateway, then the link recovery automatically attempts to connect with alternate TN799DP (C-LAN) circuit packs. The circuit packs are within the configuration of the original server or to the Survivable Remote server.

Auto fallback to the primary server

The auto fallback to primary controller feature returns a fragmented network to the primary server automatically. The fragmented networks have a number of Branch Gateways that one or more Survivable Remote servers service. This feature is applicable to all Branch Gateways. The distributed telephony switch network can be made complete by automatically migrating the gateways back to the primary server.

Survivable Remote servers

Survivable Remote servers can function as survivable call processing servers for remote or branch customer locations. Survivable Remote servers have a complete set of Communication Manager features. With the license file, Survivable Remote servers function as a survivable call processor.

If the link between the remote branch gateways and the primary controller breaks, the telephones and the gateways register with the Survivable Remote server. Survivable Remote

servers provide a backup service to the registered devices and control these devices in a license-error mode.

For more information about Survivable Remote servers, see *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

Note:

The Survivable Remote server is also known as Enhanced Local Survivability (ELS).

Survivable Core servers

Survivable Core servers provide survivability to port networks by putting the backup servers in various locations in the network of the customer. The backup servers supply service to port networks in the Simplex server fails, the Duplex server pair fails, or connectivity to the main Communication Manager server is lost. Servers for the Survivable Core server can be either Simplex or Duplex servers. The servers offer full Communication Manager functionality in the survivable mode, provided enough connectivity exists to other Avaya components. For example, endpoints, gateways, and messaging servers.

Standard Local Survivability

Standard Local Survivability (SLS) consists of a module built in to G250 Branch Gateway to provide partial backup gateway controller functionality. The gateway provides the backup function when the connection with the primary controller is lost. To provide Communication Manager functionality when no link is available to an external controller, you can use a G250 Branch Gateway with no S8300D server installed locally .

Chapter 3: Port network configurations

Communication Manager controls call processing of port networks in numerous ways. Using only Ethernet connections, control networks can be established. Voice, fax, and TTY can be transmitted over the LAN/WAN connections. Reliability with the Duplex servers can include single control and bearer networks, duplicated control networks, duplicated control and bearer networks, or a combination of reliabilities.

- Single control and bearer networks are standard reliability.
- Duplicated control networks are high reliability.
- Duplicated control and bearer networks are critical reliability.

IP port network connectivity

IP port network connectivity (IP-PNC) uses LAN or WAN connections between port networks for bearer transmission and control signaling from the server. Each port network must have either one or two control ISPI circuit packs for control signaling.

Reliability

Reliability is the capability of a Communication Manager configuration to maintain service when components within the configuration fail. For example, Ethernet switches, circuit packs, or gateways. The available reliability levels depend on whether the port networks use IP-PNC and whether the server is simplex or duplex.

Simplex server

A Simplex server provides several reliability options.

- Standard reliability

  For IP port network connectivity (IP-PNC), a Simplex server supports a single IPSI for controlling the IP-PNC PN, TN2302BP, or TN2602AP circuit packs. The circuit packs are used for the bearer network. However, TN2602AP circuit packs are implemented in the load-balancing mode only.
- Duplicated bearer reliability

  For IP-PNC, a Simplex server does not support duplicated control. However, IP-PNC PNs can have duplicated TN2602AP circuit packs to duplicate the bearer connections. Control

signaling to a PN with duplicated TN2602AP circuit packs always occurs over a direct IPSI connection to the server. A duplicated bearer network that uses TN2602AP circuit packs is implemented for each PN and does not require uniform implementation for all PNs within the configuration.

Duplex Server

A Duplex server has multiple levels of reliability.

IP port network connectivity

Reliability for PNs that use IP port network connectivity (IP-PNC) within a single Communication Manager configuration is implemented for each PN and does not require uniform implementation for other IP-PNC PNs within the configuration. In addition, duplicated bearer and duplicated control can be implemented independently of each other. Duplicated control is not required for a PN to have duplicated bearer reliability.

An IP-PNC PN can have one of the following reliability levels:

- Standard duplicated servers

  A single IPSI provides control signaling between the PN and the server. Only single or load-balancing TN2302BP or TN2602AP circuit pack pairs.

- Duplicated control

  In addition to the standard duplicated servers, duplicated IPSIs for control reside in each PN. The PN contains only single or load balancing TN2302BP or TN2602AP circuit pack pairs.

- Single control and duplicated bearer

  In addition to the standard duplicated servers, duplicated TN2602AP circuit packs reside in each PN to provide duplicated bearer.

  Note:

  Duplicated IPSI control is recommended, but not required, for duplicated bearer for IP-PNC PNs.

- Duplicated control and bearer

  In addition to the standard duplicated servers, duplicated IPSIs for control reside in each PN and duplicated TN2602AP circuit packs reside in each PN to provide duplicated bearer.

Simplex IP-PNC for the single control network

In the IP-PNC configuration, the Simplex server uses IP connections to control call processing on the PNs. The Simplex server uses an existing VoIP-ready IP infrastructure to send voice between PNs over the IP network. This solution saves customers the cost of building a

separate telephony network. In this type of configuration, all PNs are connected to the server and to each other over the customer network. You can configure up to 64 PNs in an IP-PNC network. Depending on the Ethernet switches to connect to the PNs and the PN locations, the network can require multiple Ethernet switches to support the PNs.

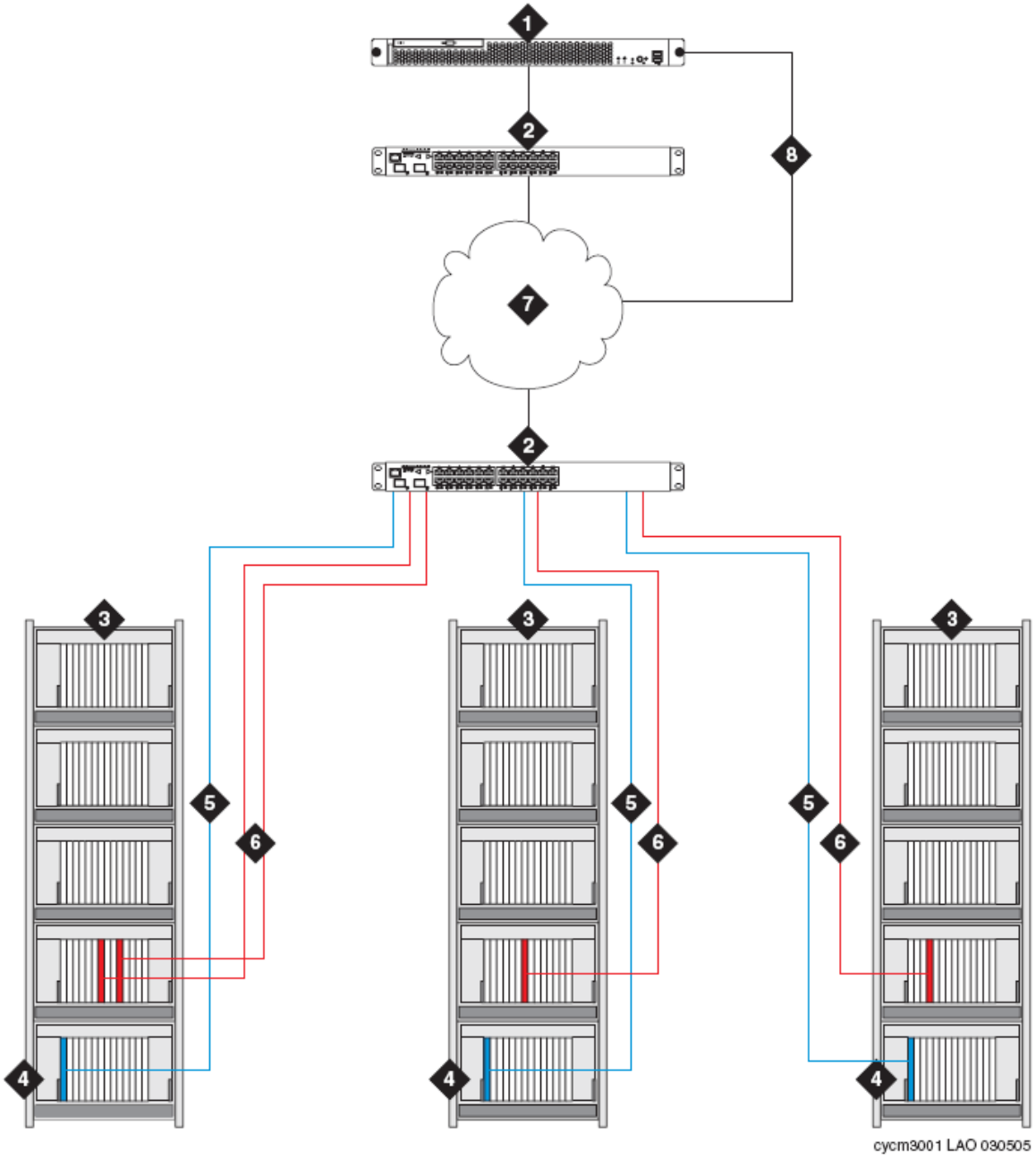
G650 Media Gateway: You can use G650 Media Gateway in an IP-PNC network. A G650 PN can consist of one to five G650 gateways in a stack connected by a TDM or LAN bus cable. One gateway that functions as control gateway in position A at the bottom of the stack contains the TN2312BP IPSI circuit pack. Only G650 Media Gateway is available for new installations. However, different migrations from older systems are supported.

IP/TDM conversion resource: Each PN must contain at least one TN2302AP IP Media Interface or TN2602AP IP Media Resource 320 circuit pack. The TN2302AP or TN2602AP circuit pack provides IP-TDM voice processing for endpoint connections between PNs. You can insert the circuit packs in any gateway in the PN. Each PN can optionally house a TN799DP C-LAN circuit pack for control of the:

- G150 Branch Gateway
- G700, G450, G430, G350, and G250 Branch Gateways
- IP endpoints
- Adjunct systems, such as messaging and firmware downloads

Ethernet connections: In the IP-PNC configuration, the Simplex server connects to the gateways through a single Ethernet switch. Each PN connects to the Simplex server through a local Ethernet switch. As a result, remote PNs in an IP-PNC configuration over WAN can require Ethernet switches in addition to the Ethernet switch that supports the Simplex server. You can administer IP connections to the Simplex server as dedicated private LAN connections or connections over the customer LAN.

Architecture of simplex server IP-PNC



Number	Description
1	Simplex server C or B.
2	Ethernet Switch. For local LAN connections, the same Ethernet switch can connect both the servers and the gateways. For remote

Number	Description
	LAN/WAN connections the remote gateway(s) must have an Ethernet switches at the remote location.
3	PNs (G650 Media Gateway or stack [shown in figure]).
4	PN control gateway in the A position in the gateway stack which contains: • A TN2312AP/BP IPSI circuit pack for IP connection to server. **Note:** For the G650 Media Gateway, the BP version of the TN2312 is required to provide environmental maintenance.
5	IPSI-to-server control network connection via Ethernet switch.
6	LAN connections of TN2302AP IP Media Interface or TN2602AP IP Media Resource 320 for IP-TDM voice processing and optional TN799DP C-LAN for control of IP endpoints **Note:** The number of TN2302AP, TN2602AP, and TN799DP circuit packs varies, depending on the number of IP endpoints, PNs, and adjunct systems. These circuit packs can be inserted into a port gateway (shown in figure) or the PN control gateway.
7	Customer LAN/WAN.
8	LAN connections of servers for remote administration.

Duplicated TN2602AP circuit packs in IP-PNC PNs

For a Simplex server, any IP-PNC PN can contain load-balancing or duplicated TN2602AP circuit packs. However, TN2602AP circuit packs do not need to be implemented uniformly within the system. PNs can either have a single TN2602AP circuit pack, load-balancing TN2602AP circuit packs, or duplicated TN2602AP circuit packs. A Simplex server can have

duplicated bearer connections although the server does not support a duplicated control network.

Circuit packs for duplicated bearer connections

For a Simplex server, each IP-PNC can contain load-balancing circuit packs, duplicated TN2602AP circuit packs, or load-balancing TN2302AP circuit packs.

PNs can have one of the following:

- A TN2302AP circuit pack
- A TN2602AP circuit pack
- A combination of TN2302AP and TN2602AP circuit packs
- Load-balancing TN2302AP circuit packs
- Load-balancing TN2602AP circuit packs
- Duplicated TN2602AP circuit packs

A Simplex server can have duplicated bearer connections even if the server does not support a duplicated control network.

Duplex IP-PNC (single control network)

In this configuration, the Duplex servers connect to one or more PNs over an Ethernet connection using either an interim Ethernet switch and a dedicated LAN connection or the customer's LAN. Each PN is connected to the Ethernet switch or LAN with a CAT5 cable to a TN2312AP/BP IP Server Interface (IPSI) card.

This solution saves customers the cost of building a separate telephony network. In this type of configuration, all PNs are connected to the customer's network and call control from the Duplex server is also sent over the customer's network. Up to 64 PNs can be configured in an IP-PNC network.

Only the G650 media gateway is available for new installations. However, because different migrations from older systems are supported, the following gateways can be used in an IP-PNC network:

- G650 media gateway

  A G650 PN can consist of one to five G650 gateways in a stack connected by a TDM/LAN bus cable. One gateway, serving as control gateway in position A at the bottom of the stack, contains the following:

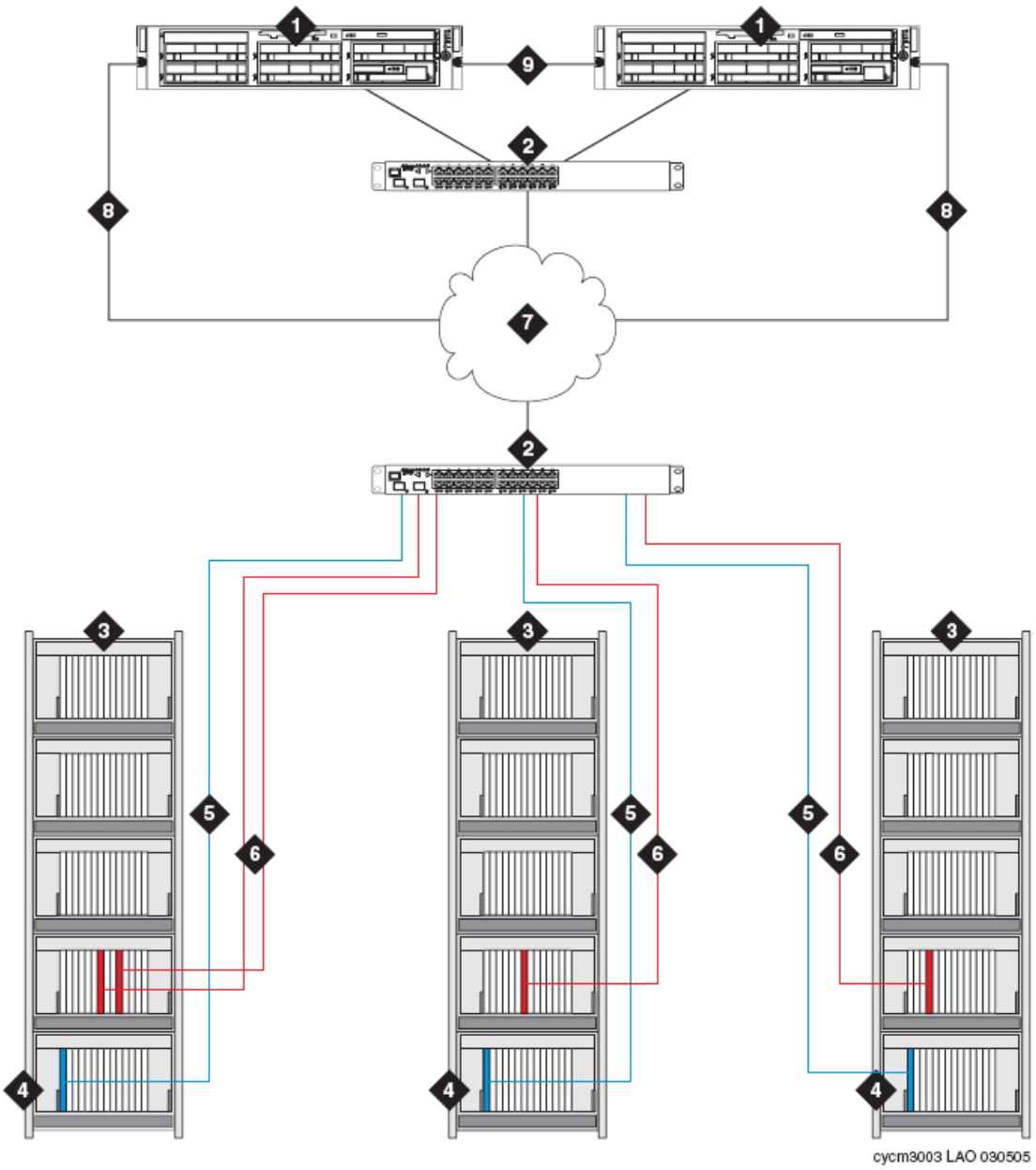
  - TN2312BP IPSI circuit pack

IP/TDM conversion resource: Each PN must contain at least one TN2302AP IP Media Interface or TN2602AP IP Media Resource 320 circuit pack. The TN2302AP or TN2602AP

circuit pack provides IP-TDM voice processing of endpoint connections between PNs. Optionally, one or more TN799DP C-LAN circuit pack can be present for control of the G150 Branch Gateway, the branch gateways (G700, G450, G430, G350, G250), IP endpoints, adjunct systems such as messaging, and firmware downloads. These circuit packs can be inserted in any gateway in the PN.

Ethernet connections: In the IP-PNC configuration, the Duplex server connects to the gateways through a single Ethernet switch. Each PN also has a connection to the network or the Duplex server through a local Ethernet switch. As a result, remote PNs in an IP-PNC configuration over a WAN, which normally requires routers to complete the connection, require their own Ethernet switches in addition to the Ethernet switch that supports the Duplex server. IP connections to the Duplex server are administered as dedicated private LAN connections or connections over the customer LAN.

Architecture of duplex IP-PNC single control network



Number	Description
1	Duplex server.
2	Ethernet Switch. For local LAN connections, the same Ethernet switch can connect both the servers and the gateways. For remote LAN/WAN connections, the remote

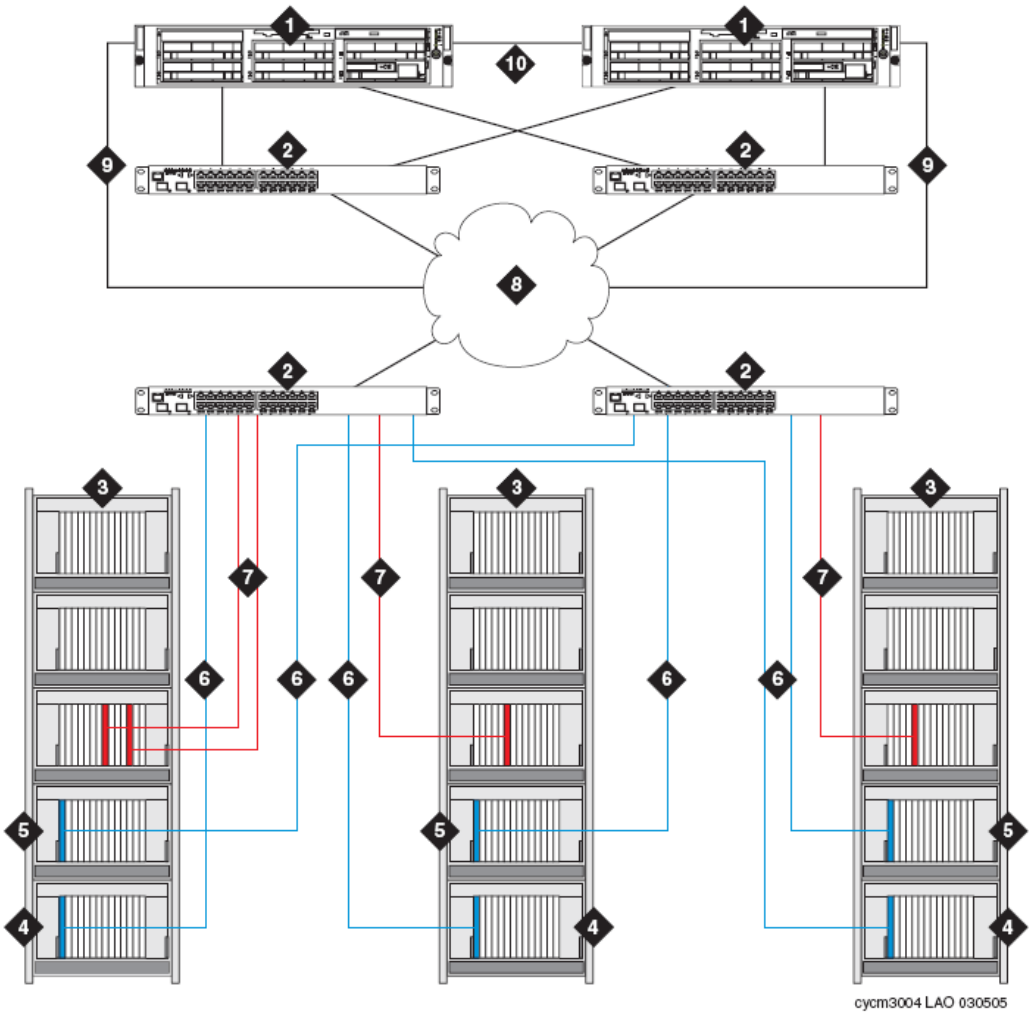
Number	Description
	gateway(s) must have an Ethernet switches at the remote location.
3	PNs (G650 Media Gateway or stack [shown in figure]).
4	PN control gateway, in the A position, which contains a TN2312AP/BP IPSI circuit pack for IP connection to server. **Note:** For each physical location of a PN or group of PNs, one PN must also contain a TN771 Maintenance circuit pack **Note:** For the G650 Media Gateway, the BP version of the TN2312 is required to provide environmental maintenance.
5	IPSI-to-server control network connection via Ethernet switch.
6	LAN connections of TN2302AP IP Media Interface or TN2602AP IP Media Resource 320 for IP-TDM voice processing and optional TN799DP C-LAN for control of IP endpoints **Note:** The number of TN2302AP, TN2602AP, and TN799DP circuit packs varies, depending on the number of IP endpoints, PNs, and adjunct systems. These circuit packs can be inserted into a port gateway (shown in figure) or the PN control gateway.
7	Customer LAN/WAN.
8	LAN connections of servers for remote administration.
9	Duplicated server links, including the link for translations memory duplication and the link for control data sharing. The link for memory duplication is implemented through the DAL2 board or (for the Duplex Server) through software duplication.

The Duplex server IP-PNC for a duplicated control network

The Duplex server IP-PNC high-reliability configuration is similar to the standard-reliability configuration, except for the following differences:

- Duplicated Ethernet switches are available with each server connected to each Ethernet switch.
- Each PN has a duplicated TN2312AP or TN2312BP IPSI circuit pack. You can connect one IPSI circuit pack in each PN through one Ethernet switch and another IPSI circuit pack through another Ethernet switch.

Architecture of duplex IP-PNC duplicated control network



Number	Description
1	Duplex server.
2	Ethernet Switch. For local LAN connections, the same Ethernet switch can connect both the servers and the gateways. For remote LAN/WAN connections, the remote gateway(s) must have an Ethernet switches at the remote location.
3	PNs (G650 Media Gateway or stack [shown in figure]).
4	PN control gateway, in the A position, which contains a TN2312AP/BP IPSI circuit pack for IP connection to server.

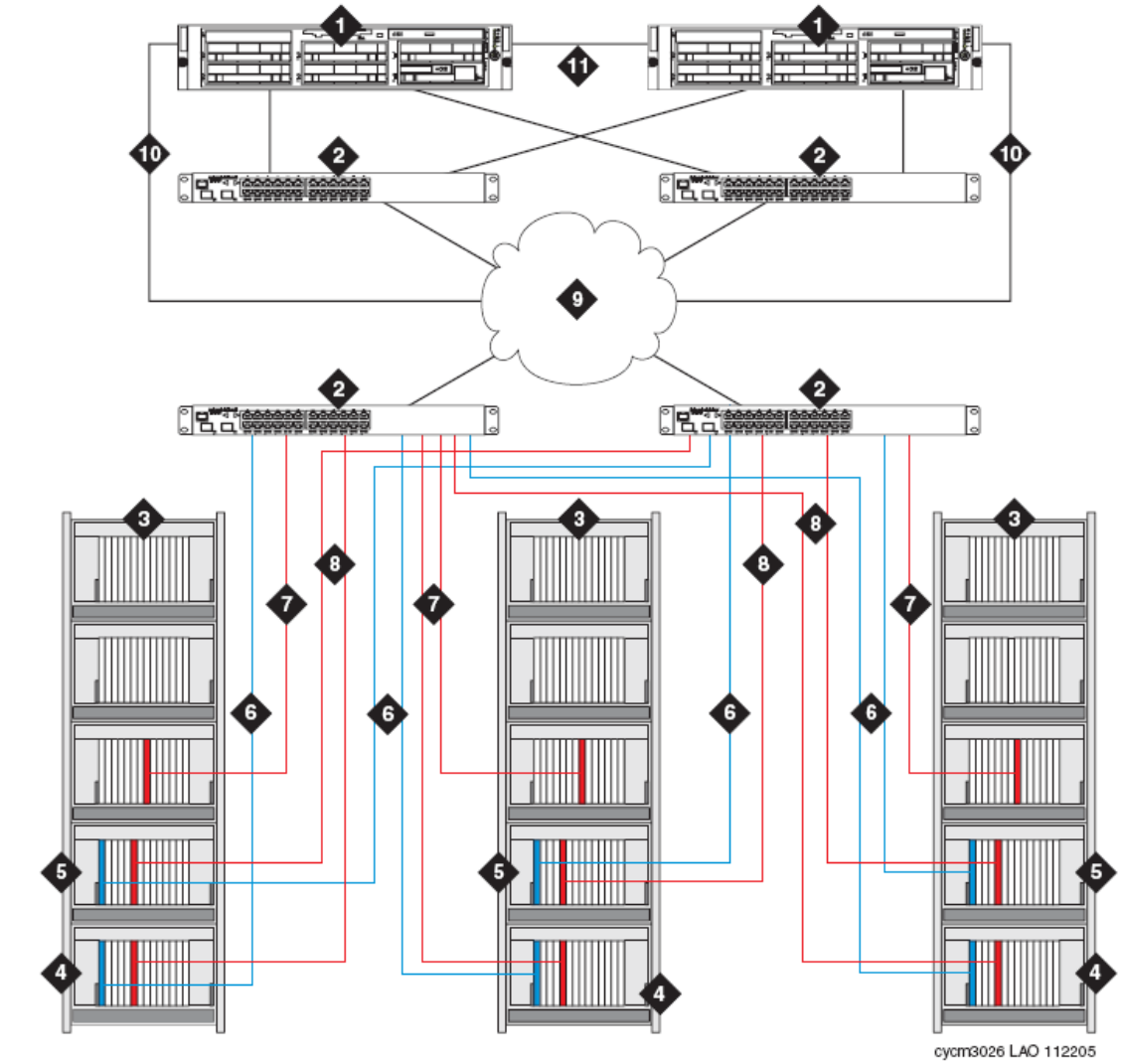
Number	Description
	Note: For the G650 Media Gateway, the BP version of the TN2312 is required to provide environmental maintenance.
5	Duplicated expansion control gateway, in the B position, which contains: A TN2312AP/BP IPSI circuit pack for IP connection to control network.
6	IPSI-to-server control network connection via Ethernet switch.
7	LAN connections of TN2302AP IP Media Interface or TN2602AP IP Media Resource 320 for IP-TDM voice processing and optional TN799DP C-LAN for control of IP endpoints. **Note:** The number of TN2302AP, TN2602AP, and TN799DP circuit packs varies, depending on the number of IP endpoints, PNs, and adjunct systems. These circuit packs can be inserted into a port gateway (shown in figure) or the PN control gateway.
8	Customer LAN/WAN.
9	LAN connections of servers for remote administration.
10	Duplicated server links, including the link for translations memory duplication and the link for control data sharing. The link for memory duplication is implemented through the DAL2 board or (for the Duplex Server) through software duplication.

The Duplex server IP-PNC for a duplicated control and bearer network connection

The Duplex server IP-PNC critical-reliability configuration is similar to the high-reliability configuration, except for the following differences:

- Each PN has duplicated TN2602AP IP Media Resource 320 circuit packs. You can connect one TN2602 circuit pack in each PN through one Ethernet switch and another TN2602 circuit pack through another Ethernet switch.
- You must install a TN771DP maintenance test circuit pack in each PN that has duplicated control and bearer network connections.

Architecture of duplex IP-PNC duplicated control and duplicated bearer network

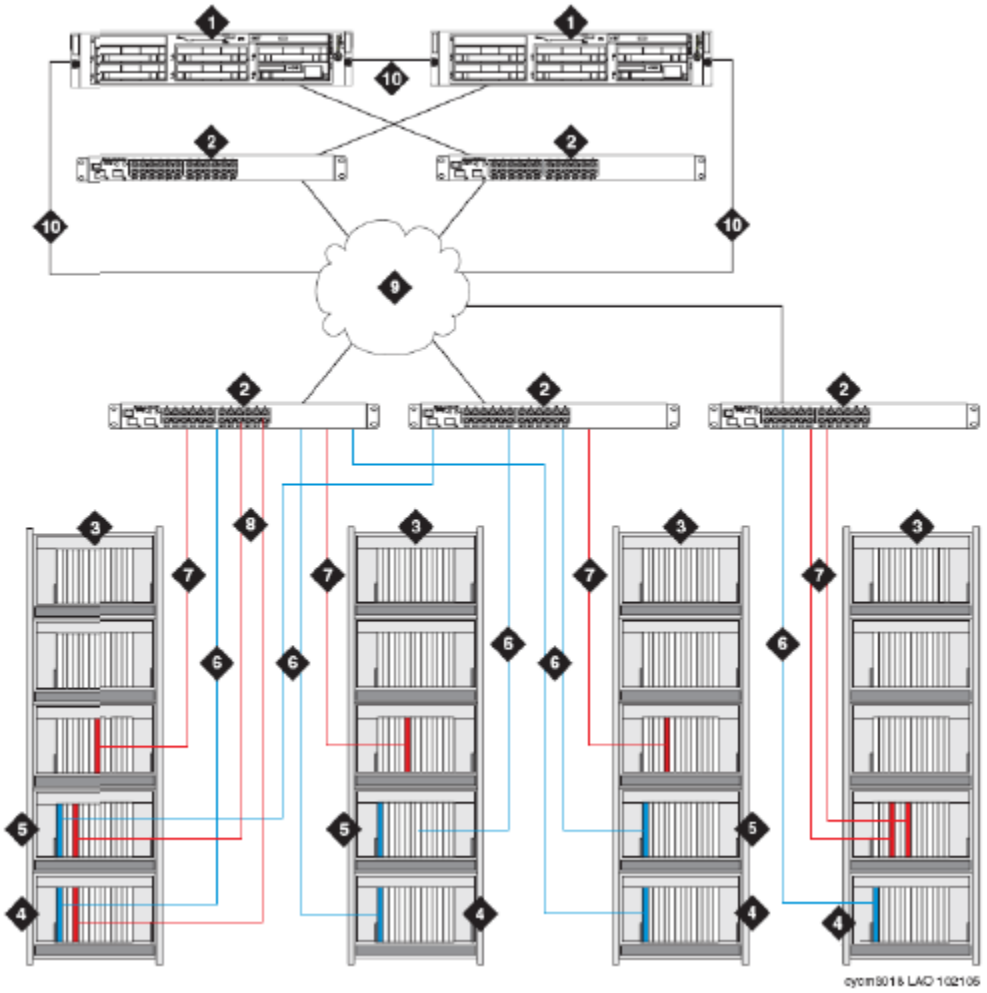


Number	Description
1	Duplex server.
2	Ethernet Switch. For local LAN connections, the same Ethernet switch can connect both the servers and the gateways. For remote LAN/WAN connections, the remote gateway(s) must have an Ethernet switches at the remote location.
3	PNs (G650 Media Gateway or stack [shown in figure]).
4	PN control gateway, in the A position, which contains: • A TN2312AP/BP IPSI circuit pack for IP connection to server. **Note:** For the G650 Media Gateway, the BP version of the TN2312 is required to provide environmental maintenance. • A TN2602AP IP Media Resource 320 for PN bearer connections over the LAN **Note:** The TN2602AP circuit pack can be placed in any gateway in the PN. However, the pair of TN2602 circuit packs should be separated between two different gateways whenever possible.
5	Duplicated expansion control gateway, in the B position, which contains: • A TN2312AP/BP IPSI circuit pack for IP connection to control network. • A TN2602AP IP Media Resource 320 for PN bearer connections over the LAN **Note:** The TN2602AP circuit pack can be placed in any gateway in the PN. However, the pair of TN2602 circuit packs should be

Number	Description
	separated between two different gateways whenever possible.
6	IPSI-to-server control network connection via Ethernet switch.
7	LAN connection of the TN799DP C-LAN for control of IP endpoints **Note:** The number of TN799DP circuit packs varies, depending on the number of IP endpoints, PNs, and adjunct systems. These circuit packs can be inserted into a port carrier (shown in figure), the PN control carrier, or the duplicated control carrier.
8	LAN connections of TN2602AP IP Media Resource 320 circuit packs for IP-TDM voice processing.
9	Customer LAN/WAN.
10	LAN connections of servers for remote administration.
11	Duplicated server links, including the link for translations memory duplication and the link for control data sharing. The link for memory duplication is implemented through the DAL2 board or (for the Duplex Server) through software duplication.

Example of IP-PNC PNs with different reliability levels

The following image illustrates a Duplex server configuration that combines duplicated control and duplicated bearer networks, duplicated control-only network, and single control network reliability configurations in an IP-PNC network. The PN with a single control network is labeled as item 11. Other PNs, items 3, have duplicated control networks.



Number	Description
1	Duplex server.
2	Ethernet Switch. For local LAN connections, the same Ethernet switch can connect both the servers and the gateways. For remote LAN or WAN connection, the remote gateway must have an Ethernet switch at the remote location.
3	IP-PNC PNs (G650 Media Gateway or stack).
4	Control gateway for PN 3, in the A position in the gateway stack. The control gateway contains: • A TN2312AP/BP IPSI circuit pack for IP connection to server.

Number	Description
5	Duplicated PN control gateway for PN3, in the B position in the gateway stack. The control gateway contains: • A TN2312AP/BP IPSI circuit pack for IP connection to control network
6	IPSI-to-server control network connection via Ethernet switch.
7	LAN connections of TN2302AP IP Media Interface or TN2602AP IP Media Resource 320 for IP-TDM voice processing and optional TN799DP C-LAN for control of IP endpoints **Note:** **NOTE**: The number of TN2302AP, TN2602AP, and TN799DP circuit packs varies, depending on the number of IP endpoints, port networks, and adjunct systems. These circuit packs can be inserted into a port carrier (shown in figure), the PN control carrier, or the duplicated control carrier.
8	Customer LAN/WAN.
9	LAN connections of servers for remote administration.
10	Duplicated server links, including the link for translations memory duplication and the link for control data sharing. The link for memory duplication is implemented through the DAL2 board or (for the Duplex Server) through software duplication.

Chapter 4: Control networks

Control networks carry the call signaling data between the call servers and the port networks. A control network is an Ethernet link between an Ethernet port on a Simplex or Duplex server and an Ethernet port on an IPSI circuit pack in a PN.

Layer 2 connectivity options

The following figures show single and duplicated control networks that use Layer 2 connectivity:

L2 Example 1: Layer 2

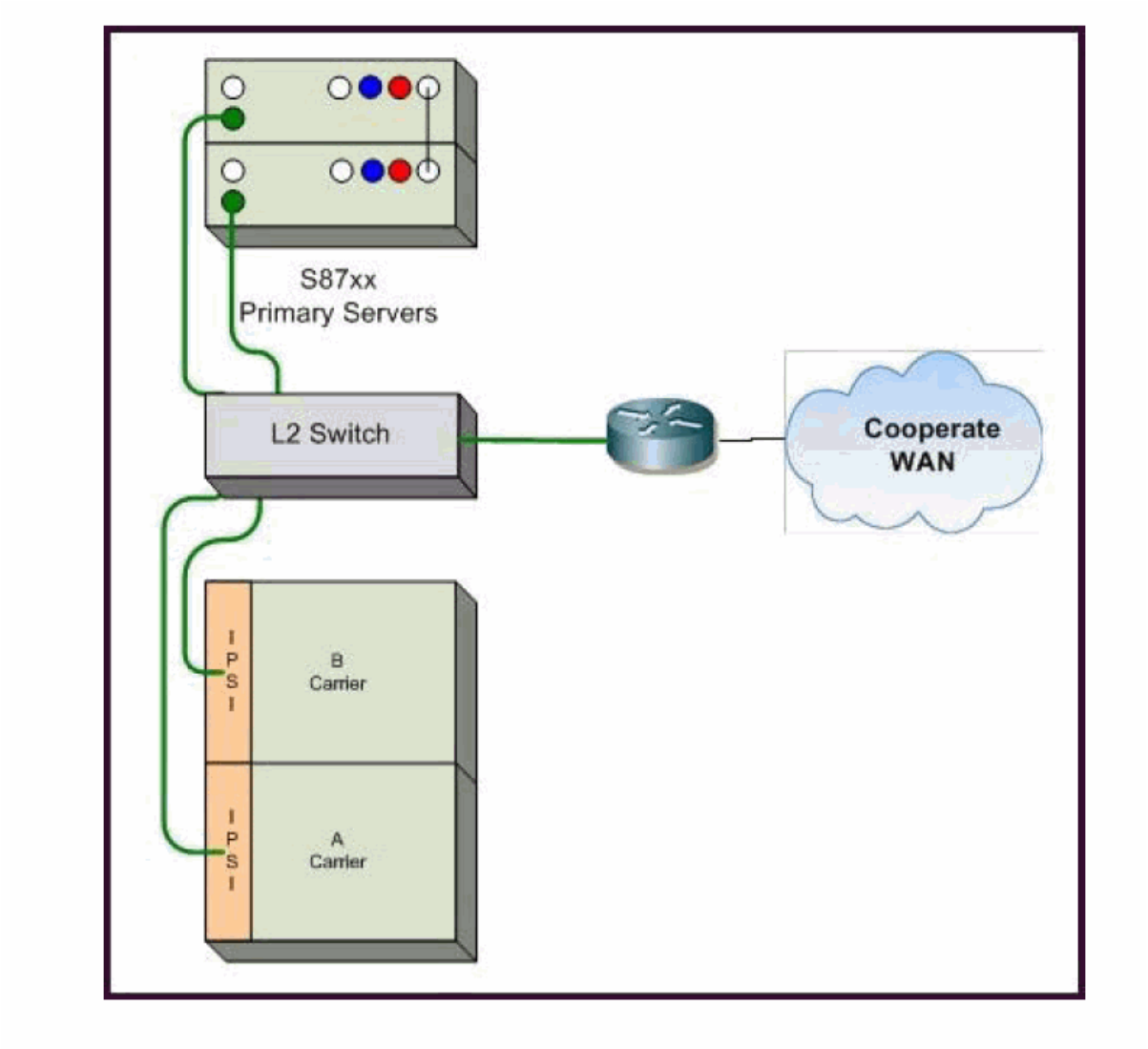


Figure 5: Layer 2 control network connectivity

L2 Example 2: Layer 2 duplicated control network

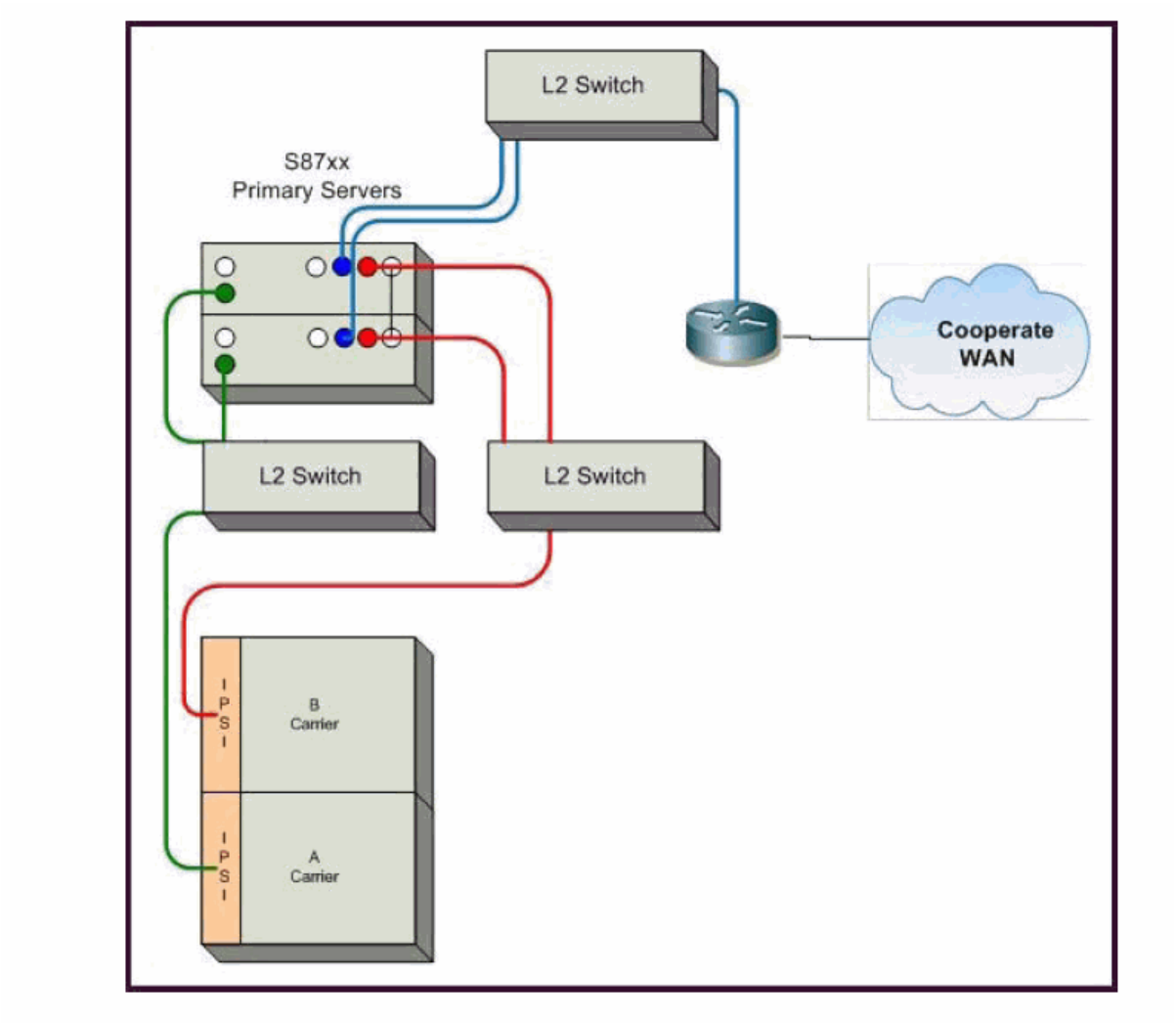


Figure 6: Layer 2 redundant control network connectivity

Layer 3 connectivity options

The following example shows a remote-backup server with Layer 3 connectivity routed over the corporate WAN.

Figure Multisite single interface shows the configuration that connects all Avaya servers and gateway interfaces to a single VLAN for each location. For the primary cluster to control the PNs at the remote site, the primary servers must have IP connectivity to the remote IPSIs. For the backup cluster to take control of the primary site PNs, the primary servers must have IP connectivity to the primary site IPSIs across the network. This design is not used frequently as for large sites the control network is separated for increased reliability.

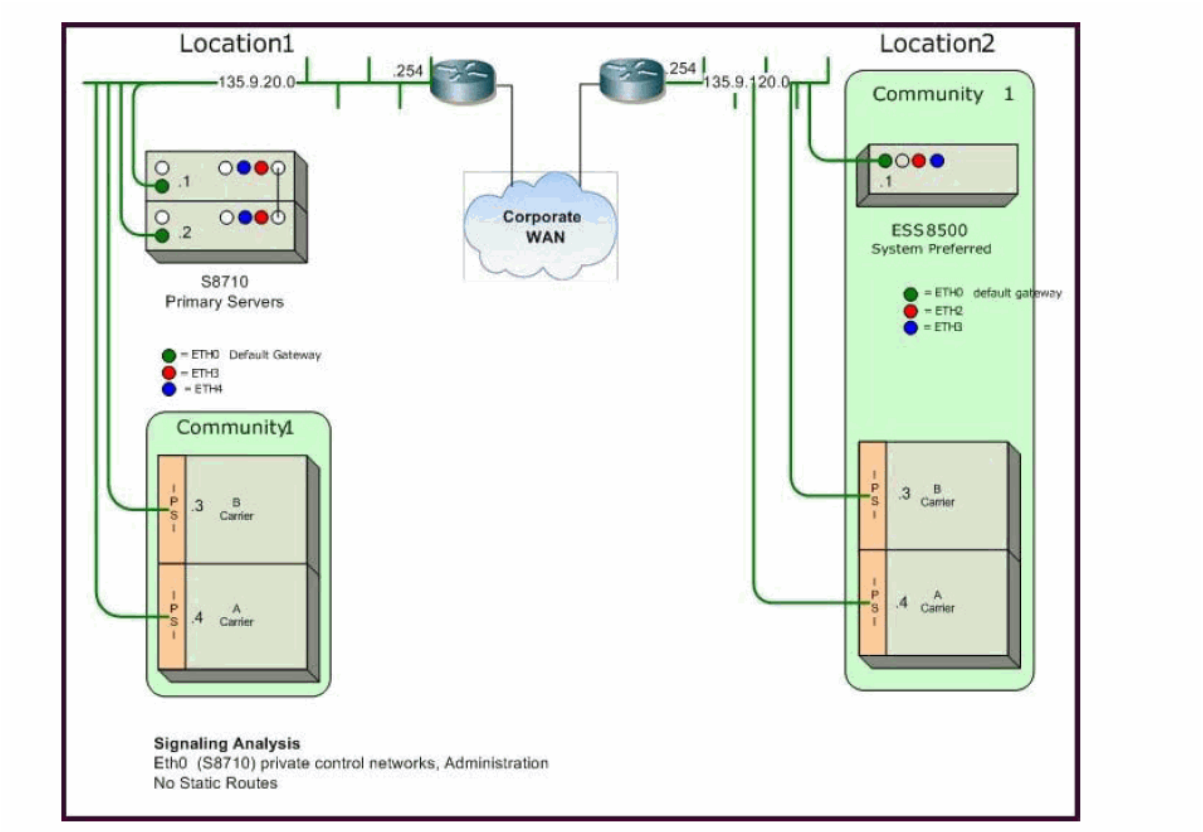


Figure 7: Multi-site single interface

Table 1: Netstat information

Destination	Gateway	Genmask	Interface
Location 1 Netstat			
135.9.20.0 (CNA, CNB)	135.9.20.1	255.255.255.0	Eth0
0.0.0.0 (Default gateway)	135.9.20.254	0.0.0.0	Eth0
Location 2 Netstat			
135.9.120.0 (CNA, CNB)	135.9.120.1	255.255.255.0	Eth0
0.0.0.0 (Default gateway)	135.9.120.254	0.0.0.0	Eth0
No static routes are required			

Advantages: Simple, no host-based static routing required.

Disadvantages: Provides no control point to protect the control connection from network conditions that results in IP packets not reaching the destinations. Using this design, the control connection can have threats, such as DoS attacks, viruses, spanning tree calculations. Any disruption in IP connectivity disrupts the TDM connections.

Control network on customer LAN

You can use routed control networks when using the control network on Customer LAN option. Control network on customer LAN (CNOCL) removed many of the IP connectivity differences. CNOCL provides enterprises with several options to create and extend control networks.

Example 1: Multi-site CNOCL using merged enterprise and control network

The *Multi-site, CNOCL (host routes)* figure and the *Multi-site, CNOCL (subnet routes)* figure show the connection of the two private control networks to the customers enterprise network, making them public. They are designated public in this case because the IP addressing of these control networks must be routable through the enterprise network.

This design has been used successfully in several Avaya deployments, but opens the control networks to all network issues experienced in the enterprise. Firewalls or strong access lists should be used to protect each site's control network, but inter-site connectivity cannot truly be protected. The use of the third interface connecting to the enterprise infrastructure for management is no longer necessary, and can be collapsed on the one of the other two networks.

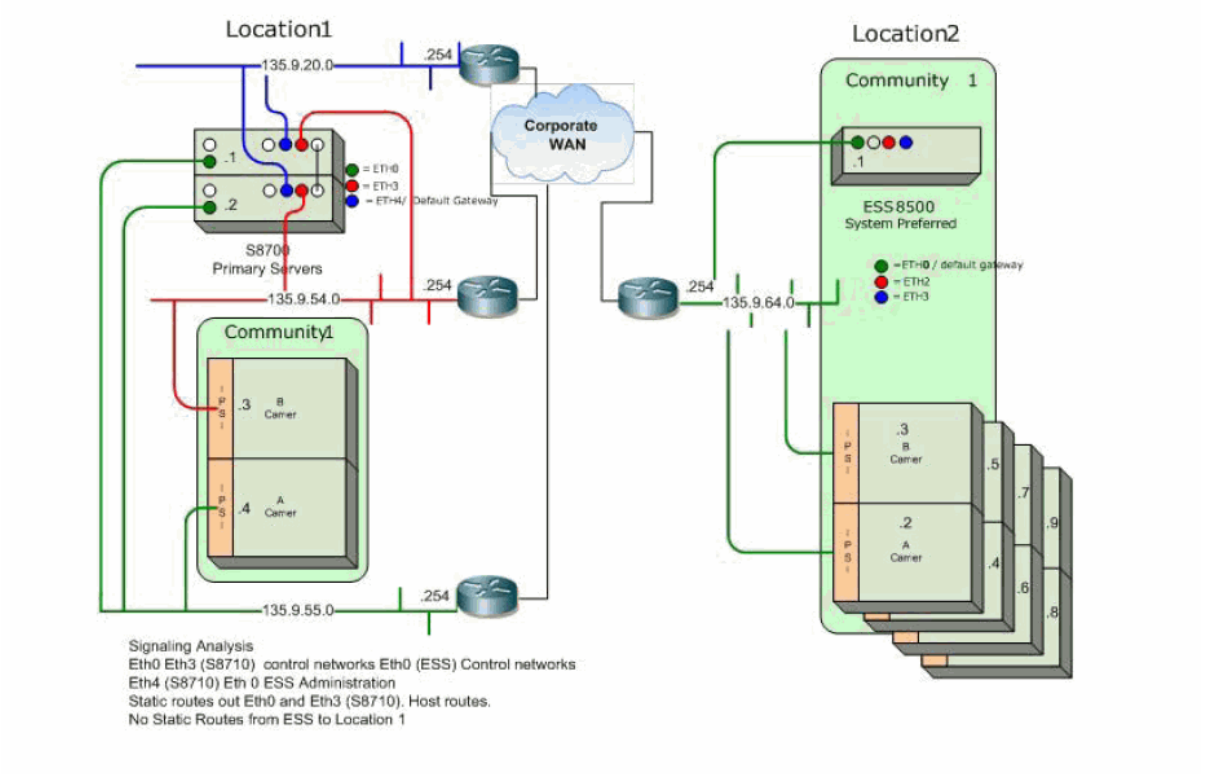


Figure 8: Multi-site, CNOCL (host routes)

Table 2: Netstat information

Destination	Gateway	Genmask	Interface
Location 1			
135.9.20.0 (LAN)	135.9.20.1	255.255.255.0	Eth4
135.9.54.0 (CNB)	135.9.54.1	255.255.255.0	Eth3
135.9.55.0 (CNA)	135.9.55.1	255.255.255.0	Eth0
135.9.64.3	135.9.54.254	255.255.255.255	Eth3
135.9.64.5	135.9.54.254	255.255.255.255	Eth3
135.9.64.7	135.9.54.254	255.255.255.255	Eth3
135.9.64.9	135.9.54.254	255.255.255.255	Eth3
135.9.64.2	135.9.55.254	255.255.255.255	Eth0
135.9.64.4	135.9.55.254	255.255.255.255	Eth0
135.9.64.6	135.9.55.254	255.255.255.255	Eth0
135.9.64.8	135.9.55.254	255.255.255.255	Eth0
0.0.0.0 (Default gateway)	135.9.20.254	0.0.0.0	Eth4
Location 2			
135.9.64.0	0.0.0.0	255.255.255.0	Eth0
0.0.0.0 (Default gateway)	135.9.120.254	0.0.0.0	Eth0

Table 3: Static (host) routes

Destination	Subnet Mask	Gateway	Interface
Location 1			
135.9.64.2	255.255.255.255	135.9.55.254	0
135.9.64.3	255.255.255.255	135.9.54.254	3
135.9.64.4	255.255.255.255	135.9.55.254	0
135.9.64.5	255.255.255.255	135.9.54.254	3
135.9.64.6	255.255.255.255	135.9.55.254	0
135.9.647	255.255.255.255	135.9.54.254	3
135.9.64.8	255.255.255.255	135.9.55.254	0
135.9.64.9	255.255.255.255	135.9.54.254	3
Location 2 No static routes required			

Advantages: Provides a control point to limit traffic on the control network. With additional Ethernet switches, it can provide protection against utilization failures and spanning tree

recalculations. TDM connections can continue during specific network failures. No host-based static routing required.

Disadvantages: Requires additional VLANs and/or dedicated switches and router interfaces.

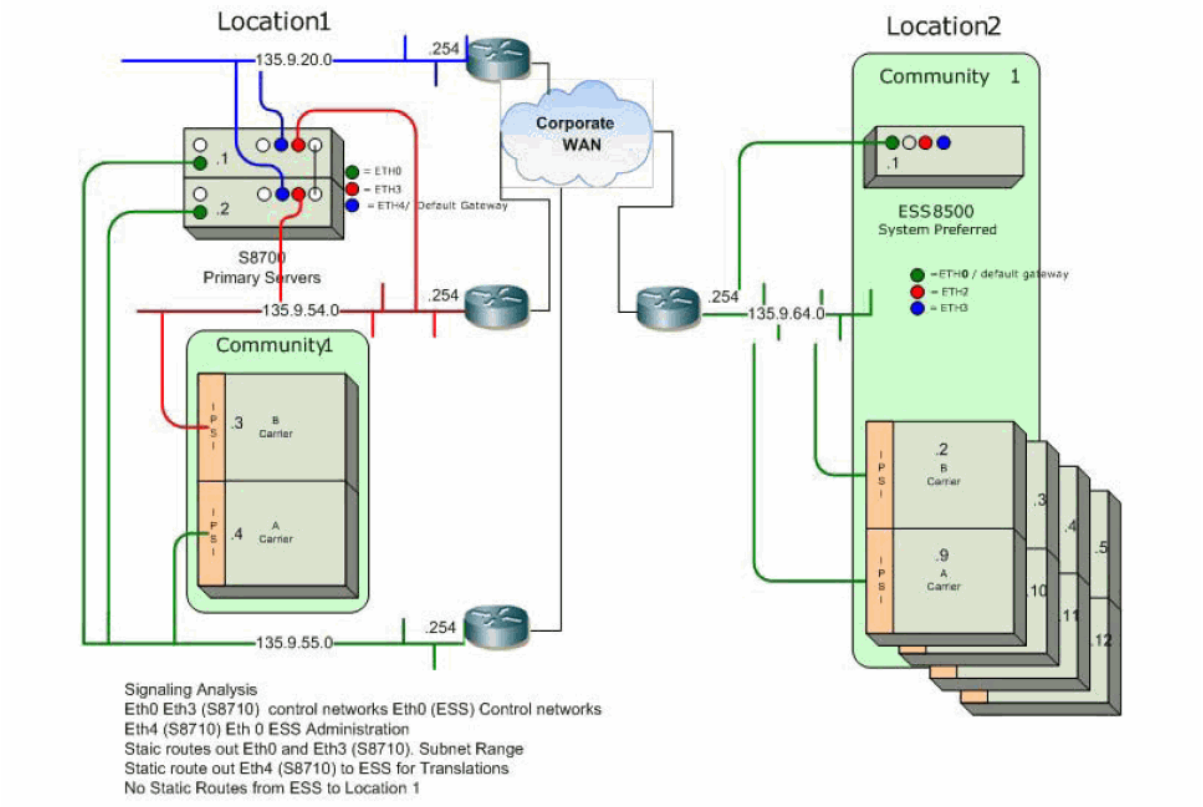


Figure 9: Multi-site, CNOCL (subnet routes)

Table 4: Netstat information

Destination	Gateway	Genmask	Interface
Location 1			
135.9.20.0 (LAN)	135.9.20.1	255.255.255.0	Eth4
135.9.54.0 (CNB)	135.9.54.1	255.255.255.0	Eth3
135.9.55.0 (CNA)	135.9.55.1	255.255.255.0	Eth0
135.9.64.0	135.9.54.254	255.255.255.248	Eth3
135.9.64.8	135.9.55.254	255.255.255.248	Eth0
135.9.64.1	135.9.20.254	255.255.255.255	Eth4
0.0.0.0 (Default gateway)	135.9.20.254	0.0.0.0	Eth4
Location 2			
135.9.64.0 (LAN)	0.0.0.0	255.255.255.0	Eth0

Destination	Gateway	Genmask	Interface
0.0.0.0 (Default gateway)	135.9.120.254	0.0.0.0	Eth0

Table 5: Static routes

Destination	Subnet Mask	Gateway	Interface
Location 1			
135.9.64.0	255.255.255.248	135.9.54.254	3
135.9.64.8	255.255.255.248	135.9.55.254	0
135.9.64.1	255.255.255.255	135.9.20.254	4
Location 2 No static routes required			

Advantages: Provides a control point to limit traffic on the control network. Uses the enterprise's existing network infrastructure.

Disadvantages: TDM connections cannot continue during most network failures. Static routing is required on both Main and MBS/Survivable Core servers. Multiple interfaces to the enterprise network can become complex to administer. Changes in network architecture will have to be synchronized with changes in the static route table, and will be service-affecting.

Chapter 5: Converged Networks

Voice over IP converged networks

Until recently, voice, video, and data were delivered over separate, single-purpose networks. A converged network brings voice, data, and video traffic together on a single IP network. Avaya's VoIP technology provides a cost-effective and flexible way of building enterprise communications systems through a converged network.

Some of the flexible elements of a converged network include:

- Separation of call control and switching functions. See *Separation of Bearer and Signaling Job Aid*, 555-245-205
- Different techniques for handling data, voice, and FAX
- Communications standards and protocols for different network segments
- Constant and seamless reformatting of data for differing media streams

Digital data and voice communications superimposed in a converged network compete for the network bandwidth, or the total information throughput that the network can deliver. Data traffic tends to require significant network bandwidth for short periods of time, while voice traffic demands a steady, relatively constant transmission path. Data traffic can tolerate delays, while voice transmission degrades, if delayed. Data networks handle data flow effectively, but when digitized voice signals are added to the mix, networks must be managed differently to ensure constant, real-time transmission needed by voice.

Network assessment

Even if your network performs acceptably, adding VoIP taxes network resources and performance, because VoIP requires dedicated bandwidth and is more sensitive to network problems than data applications alone. Many customer IP infrastructures appear to be stable and perform at acceptable levels, but have performance and stability issues that create problems for Avaya VoIP Solutions. While a customer network can appear to be ready to support full-duplex VoIP applications, Avaya cannot assure performance and quality without a network assessment.

The network assessment services for Avaya VoIP consist of 2 phases:

- Basic Network Assessment — is a high-level LAN/WAN infrastructure evaluation that determines the suitability of an existing network for VoIP.
- Detailed Network Assessment — is typically the second phase in the Network Assessment for IP Telephony solutions.

  The detailed network assessment takes information gathered in the basic network assessment, performs problem diagnosis, and provides functional requirements for the network to implement Avaya VoIP.

For more information, see

- Network assessment offer in *Avaya Aura® Solution Design Considerations and Guidelines*, 03-603978.
- Avaya Communication Solutions and Integration (CSI)

  Avaya Communication Solutions and Integration (CSI) supports a portfolio of consulting and engineering offers to help plan and design voice and data networks, including:

  - IP Telephony
  - Data Networking Services
  - Network Security Services.

  You can contact Avaya CSI:

  - On the Web -- http://csi.avaya.com.
  - by email: bcsius@avaya.com
  - by telephone: +1 866 282 9266
- http://netassess.avaya.com for a description of the Avaya network assessment policy. Note: this link is available only from within the Avaya corporate network.

VoIP hardware

This section contains descriptions and administration information for the following circuit packs and media modules:

- Universal DS1 circuit packs and MM710 T1/E1Media Module on page 65
- TN799DP Control LAN on page 68
- TN2302AP IP Media Processor on page 72
- TN2602AP IP Media Resource 320 on page 73
- TN2312BP IP Server Interface (IPSI) on page 77
- MM760 VoIP Media Module on page 81

Universal DS1 circuit packs and MM710 T1/E1Media Module

The TN464HP/TN2464CP circuit packs and the MM710 Media Module (version 3 and later) have the same functionality as other DS1 circuit packs with the addition of echo cancellation circuitry, which offers echo cancellation tail lengths of up to 96 milliseconds (ms). The TN574, TN2313, and TN2464 DS1 circuit packs do not support echo cancellation.

The TN464HP/TN2464CP and MM710 are intended for users who encounter echo over circuits connected to the Direct Distance Dialing (DDD) network. Echo is most likely to be noticeable when Communication Manager is configured for ATM, IP, and wideband. With these configurations, the delay between the primary signal and the echoed signal is greater than with a TDM configuration. In addition, echo can occur on system interfaces to local service providers that do not routinely install echo cancellation equipment in all their circuits.

Echo cancellation is a software right-to-use feature that supports voice channels, and is not intended for data. When a data call is received, these circuit packs detect a modem tone and turn off echo cancellation for the duration of the data call.

Working with echo cancellation

About this task

You can see if the echo cancellation is enabled for TN464HP/TN2464CP circuit packs and MM710 T1/E1 Media Modules on the system-parameters customer-options screen.

Procedure

1. Type **`display system-parameters customer-options`**.
2. Ensure that the following fields are complete:
   - **Maximum Number of DS1 Boards with Echo Cancellation**: Specifies the number of DS1 boards that have echo cancellation turned on.
   - **DS1 Echo Cancellation**: If the value of this field is **y**, echo cancellation is enabled.

     Note:

     The system can display these fields on different pages of the screen.
3. Exit the screen.

Echo cancellation on the DS1 circuit pack or MM710 media module

Note:

Any changes made to the echo cancellation settings on the DS1 Circuit Pack screen take effect immediately.

The DS1 Circuit Pack screen for the TN464HP/TN2464CP circuit packs and MM710 media module has fields to support echo cancellation: **Echo Cancellation**, **EC Direction**, and **EC Configuration**. The **Echo Cancellation** field displays when the Echo Cancellation feature is activated on the System-Parameters Customer Options screen. The **EC Direction** and **EC Configuration** fields display when the **DS1 Echo Cancellation** field is enabled.

- **EC Direction** determines the direction from which echo will be eliminated, ether inward or outward.
- **EC Configuration** is the set of parameters used when cancelling echo.

  This information is stored in firmware on the UDS1 circuit pack.

Administering the DS1 circuit pack and MM710 media module

Procedure

1. Type **add ds1 <port>**, where **<port>** is the location of the DS1 circuit pack, or the MM710 media module.
2. Press `Enter`.

   The system displays the DS1 Circuit Pack screen.
3. In the **Echo Cancellation** field, type `y` to enable echo cancellation on the Universal DS-1 circuit pack.
4. In the **Echo Direction** field, type `inward` or `outward` indicating the direction of the echo that is to be cancelled.
5. In the **EC Configuration** field, type digits between 1 to 15 indicating the set of parameters used for echo cancellation.

   Note:

   The system displays the **EC Configuration** field on the screen only when the **Echo Cancellation** field is set to `y`.

Result

For more information about these fields, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

Echo cancellation on trunks

Note:

Changes to echo cancellation settings on the Trunk Features screen do not take effect until after a port or trunk group is busied-out/released, or the SAT command **`test trunk group`** is performed, or periodic maintenance is run.

Echo cancellation is turned on or off on a per trunk-group basis using the **`change trunk-group`** command. If the trunk group field, **DS1 Echo Cancellation** is **`y`**, echo cancellation is applied to every TN464HP/TN2464CP trunk member in that trunk group. The echo cancellation parameters used for a given trunk member are determined by the **EC Configuration** number administered on the DS1 Circuit Pack screen for that specific trunk's board.

Echo cancellation applies to voice channels and supports echo cancellation on the following trunk group types:

- CO
- TIE
- ISDN-PRI
- FX
- WATS
- DID
- DIOD
- DMI-BOS
- Tandem
- Access
- APLT

Administration of echo cancellation on a trunk group is done on the TRUNK FEATURES screen.

Administering a trunk group for echo cancellation

Procedure

1. Type **`change trunk-groupn`**, where **`n`** is the trunk group number.

2. Go to the Trunk Features page.

   Note:

   The system displays the fields on the screen depending on the trunk group type.

3. In the **DS1 Echo Cancellation** field, type **y** to enable echo cancellation on a per trunk group basis.
4. Save the changes.

TN799DP Control LAN

Systems in a private network are interconnected by both tie trunks (for voice communications) and data links (for control and transparent feature information). Various DS1, IP, and analog trunk circuit packs provide the voice-communications interface. For TCP/IP connectivity, the data-link interface is provided by a TN799DP Control LAN (C-LAN) circuit pack. (For more information about this VoIP transmission hardware, see VoIP-transmission hardware on page 29 of the *Networking Overview* chapter.)

The C-LAN handles the data-link signaling information in one of two configurations: Ethernet, or point-to-point (PPP). The C-LAN circuit pack has one 10/100baseT ethernet connection and up to 16 DS0 physical interfaces for PPP connections. C-LAN also extends ISDN capabilities to csi models by providing packet-bus access.

- In the Ethernet configuration, the C-LAN passes the signaling information over a separate TCP/IP network, usually by means of a hub or Ethernet switch.

  Use an Ethernet switch for optimal performance. For this configuration, install the C-LAN circuit pack and connect the appropriate pins of the C-LAN I/O field to the hub or Ethernet switch.

- In the PPP configuration, the C-LAN passes the data-link signaling to the DS1 for inclusion in the same DS1 bit stream as the DCS voice transmissions.

  For this configuration, install the C-LAN circuit pack; no other connections are needed. The appropriate DS1 circuit packs must be installed, if they are not already present.

Physical addressing for the C-LAN board

The Address Resolution Protocol (ARP) on the C-LAN circuit pack relates the 32-bit IP address configured in software to the 48-bit MAC address of the C-LAN circuit pack. The MAC address is burned into the board at the factory. The C-LAN board has an ARP table that contains the IP addresses associated with each hardware address. This table is used to route messages

across the network. Each C-LAN board has one MAC address, one Ethernet address, and up to 16 PPP addresses.

IP addressing techniques for the C-LAN board

The C-LAN supports both Classless Inter-domain Routing and Variable-Length Subnet Masks. These addressing techniques provide greater flexibility in addressing and routing than class addressing alone.

Installing the TN799DP C-LAN

About this task

TCP/IP connections (Ethernet or PPP) require a TN799DP C-LAN circuit pack, unless your system has embedded Ethernet capabilities. Before you install the C-LAN circuit pack, be sure you understand the requirements of your LAN. For information about LAN requirements for VoIP, go to http://www.extremenetworks.com/LIBRARIES/Avaya/AvayaIPvoiceQualityNetworkRequirements.pdf and look in the white paper titled *Avaya IP Voice Quality Network Requirements (EF-LB1500)*.

The following steps describe installation for the TN799DP C-LAN.

Procedure

1. Determine the carrier/slot assignments of the circuit packs to be added.
   You can insert the C-LAN circuit pack into any port slot.
2. Insert the circuit packs into the slots specified in step 1.

Note:

You do not need to switch off the cabinet to install a C-LAN circuit pack.

Installing C-LAN cables to a hub or ethernet switch

About this task

In the Ethernet configuration, the C-LAN passes the signaling information over a separate TCP/IP network, usually by means of a hub or Ethernet switch. Connect the appropriate pins of the C-LAN I/O field to the hub or Ethernet switch.

See Cable connection for C-LAN connectivity on page 70.

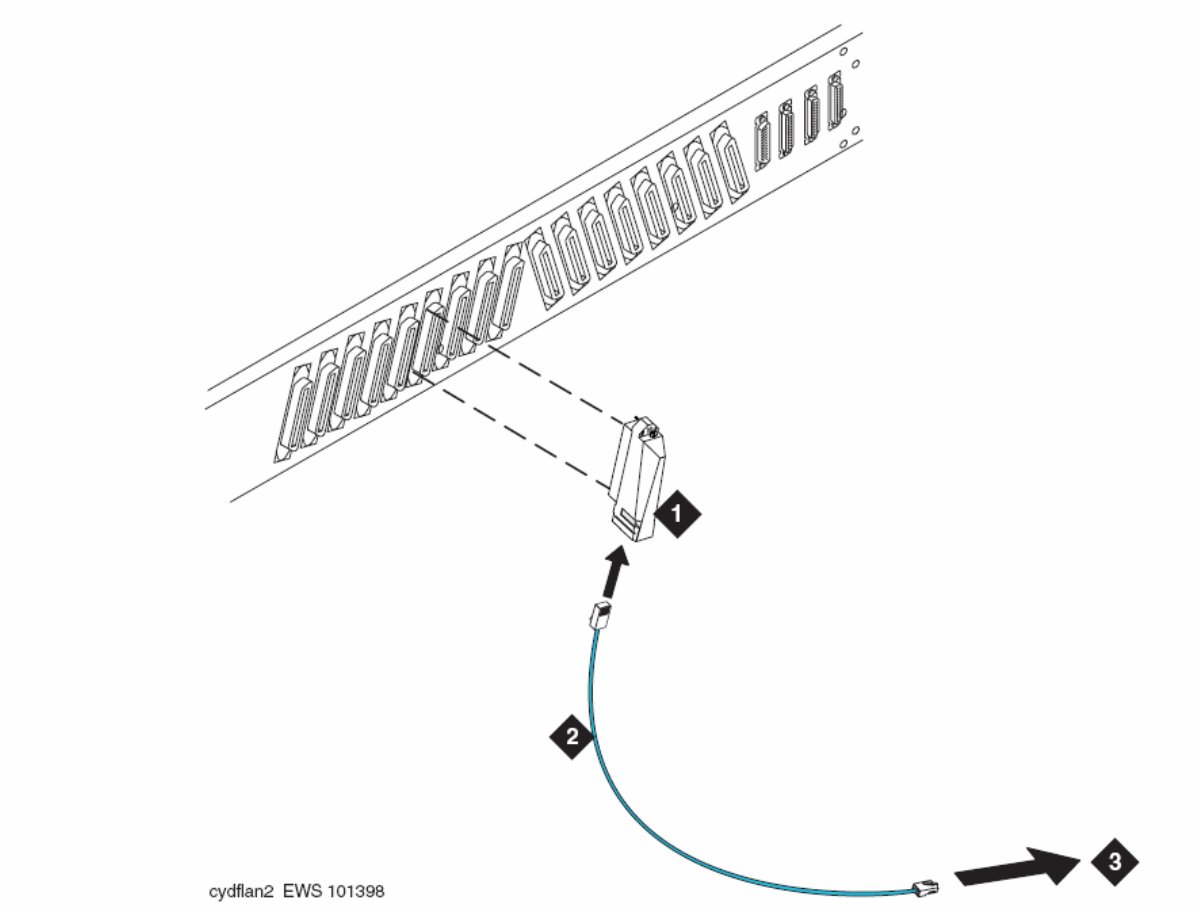
Procedure

1. Connect the 259A connector to the backplane connector of the port slot containing the C-LAN circuit pack.

2. Connect the Category 5 UTP cable between the 259A connector and a hub or Ethernet switch.

   This connects port 17 on the C-LAN circuit pack to the LAN.

Cable connection for C-LAN connectivity



Name	Description
1	259A Connector
2	Category 5 UTP Cable (max length 100m)
3	Ethernet switch

LAN default gateway

On LANs that connect to other networks or subnetworks, define a default gateway. The default gateway node is a routing device that is connected to different (sub)networks. Any packets addressed to a different (sub)network, and for which no explicit IP route is defined, are sent to the default gateway node.

You must use the IP Interfaces screen to administer a node (C-LAN port, PROCR or IP Interface port) as the default gateway.

The default node on the Node Names screen is a display-only entry with IP address 0.0.0.0. It acts as a variable that takes on unknown addresses as values. When the default IP route is set up, any address not known by the C-LAN is substituted for the default address in the default IP route, which uses the router as the default gateway.

Alternate Gatekeeper and C-LAN load balancing

Alternate Gatekeeper gives IP endpoints a list of available C-LAN circuit packs. Alternate Gatekeeper addresses and C-LAN load-balancing spread IP endpoint registration across more than one C-LAN circuit pack. The C-LAN load-balancing algorithm allocates endpoint registrations within a network region to the C-LAN with the least number of sockets in use. This increases system performance and reliability.

If registration with the original C-LAN circuit pack IP address is successful, the software sends back the IP addresses of all the C-LAN circuit packs in the same network region as the IP endpoint. If the network connection to one C-LAN circuit pack fails, the IP endpoint re-registers with a different C-LAN. If the system uses network regions based on IP address, the software also sends the IP addresses of C-LANs in interconnected regions. These alternate C-LAN addresses are also called *gatekeeper* addresses. These addresses can also be used if the data network carrying the call signaling from the original C-LAN circuit pack fails.

IP Telephones can be programmed to search for a gatekeeper independently of load-balancing. The IP Telephone accepts gatekeeper addresses in the message from the Dynamic Host Configuration Protocol (DHCP) server or in the script downloaded from the Trivial File Transfer Protocol (TFTP) server. If the telephone cannot contact the first gatekeeper address, it uses an alternate address. If the extension and password is rejected by the first gatekeeper, the IP Telephone contacts the next gatekeeper. The number of gatekeeper addresses the telephone accepts depends on the length of the addresses administered on the DHCP server.

Note:

A single Alternate Gatekeeper list is typically used in configurations with multiple servers. In this case, the DHCP server sends the same Alternate Gatekeeper list to all IP endpoints, but a given IP endpoint might be unable to register with some of the gatekeepers in the list and a registration attempt to those gatekeepers will be rejected.

C-LAN load balancing and alternate gatekeeper addresses require IP stations that accept multiple IP addresses, such as:

- IP telephone
- IP Softphone
- Avaya IP Agent

Endpoint capabilities

Table 6: Endpoint capabilities

Endpoint	Number of Gatekeepers	Settings
IP Telephone	1 8 10 72	Default - DNS name AvayaCallServer, or manually, one fixed IP address Through DHCP - DNS names or fixed IP addresses. DHCP limits all options to a total of 255 bytes. Through TFTP - DNS names or fixed IP addresses. TFTP overwrites any gatekeepers provided by DHCP Fixed IP addresses from Communication Manager. Communication Manager 2.0 and later supersedes any gatekeeper address provided previously.
IP Softphone R5	30	Manually through options or properties of the IP Softphone after it is installed.
IP Agent R3	30	Manually through options or properties of the IP agent after it is installed, or from Communication Manager.

Note:

DHCP servers send a list of alternate gatekeeper and C-LAN addresses to the IP Telephone endpoint. It is possible for a hacker to issue a false request and thereby obtain IP addresses from the DHCP server. However, the alternate gatekeeper IP addresses will only be sent to an endpoint that successfully registers.

TN2302AP IP Media Processor

Use the TN2302AP IP Media Processor to transmit voice and FAX data (non-DCS signaling) over IP connections, and for H.323 multimedia applications in H.323 V2 compliant endpoints.

The TN2302AP IP Media Processor provides port network connectivity for an IP-connected configuration. The TN2302AP IP Media Processor includes a 10/100BaseT Ethernet interface

to support H.323 endpoints for IP trunks and H.323 endpoints, and its design improves voice quality through its dynamic jitter buffers.

The TN2302AP IP Media Processor additionally performs the functions:

- Echo cancellation
- Silence suppression
- DTMF detection
- Conferencing

It supports the following codecs, FAX detection for them, and conversion between them:

- G.711 (mu-law or a-law, 64Kbps)
- G.723.1 (6.3Kbps or 5.3Kbps audio)
- G.729 (8Kbps audio)

TN2302AP transmission interface

The TN2302AP IP Media Processor provides improved voice quality through its dynamic jitter buffers. The TN2302AP's digital signal processors (DSPs), by default, insert 5.0 dB of loss in the signal from the IP endpoints, and insert 5.0 dB of gain in the signal to the IP endpoints. System administrators can administer loss/gain, based on country code on the terminal-parameters screen.

TN2302AP hairpinning

The TN2302AP IP Media Processor supports 64 ports of shallow hairpin. IP packets that do not require speech codec transcoding can be looped back at the UDP/IP layers with a simple change of addressing. This reduces delay and leaves DSP resources available.

TN2302AP ports

The TN2302AP IP Media Processor is a service circuit pack, not a trunk circuit pack. Therefore, an H.323 tie trunk cannot be used for facility test calls. Use the ping command to test the TN2302AP ports.

TN2602AP IP Media Resource 320

The TN2602AP IP Media Resource 320 provides high-capacity voice over Internet protocol (VoIP) audio access to the switch for local stations and outside trunks. The IP Media Resource 320 provides audio processing for the following types of calls:

- TDM-to-IP and IP-to-TDM
- IP-to-IP

The TN2602AP IP Media Resource 320 circuit pack has two capacity options, both of which are determined by the license file installed on Communication Manager:

- 320 voice channels, considered the standard IP Media Resource 320
- 80 voice channels, considered the low-density IP Media Resource 320

The port network can hold only two TN2602AP circuit packs.

Note:

The TN2602AP IP Media Resource 320 is not supported in CMC1 and G600 Branch Gateways.

Load balancing

Up to two TN2602AP circuit packs can be installed in a single port network for load balancing The TN2602AP circuit pack is also compatible with and can share load balancing with the TN2302 and TN802B IP Media Processor circuit packs. Actual capacity can be affected by a variety of factors, including the codec used for a call and fax support.

Note:

When two TN2602AP circuit packs, each with 320 voice channels, are used for load balancing within a port network, the total number of voice channels available is 484, because 484 is the maximum number of time slots available for a port network.

Bearer duplication

Two TN2602AP circuit packs can be installed in a single port network (PN) for duplication of the bearer network. In this configuration, one TN2602AP is an active IP media processor and one is a standby IP media processor. If the active media processor, or connections to it, fail, active connections failover to the standby media processor and remain active. This duplication prevents active calls in progress from being dropped in case of failure. The interchange between duplicated circuit packs affects only the PN in which the circuit packs reside.

Note:

The 4606, 4612, and 4624 IP telephones do not support the bearer duplication feature of the TN2602AP circuit pack. If these telephones are used while an interchange from the active to the standby media processor is in process, then calls might be dropped.

Virtual IP and MAC addresses to enable bearer duplication

Duplicated TN2602AP circuit packs in a PN share a virtual IP and virtual MAC address. These virtual addresses are owned by the currently-active TN2602. In addition to the virtual IP address, each TN2602 has a “real” IP address. All bearer packets sent to a PN that contains duplicated TN2602AP circuit packs, regardless of whether the packets originate from TN2602s in other PNs or from IP telephones or gateways, are sent to the virtual IP address of the TN2602 pair in that PN. Whichever TN2602AP circuit pack is active is the recipient of those packets.

When failover to the standby TN2602 occurs, a negotiation between TN2602s to determine which TN2602 is active and which is standby takes place. State-of-health, call state, and encryption information is shared between TN2602s during this negotiation. The newly-active TN2602AP circuit pack sends a gratuitous address resolution protocol (ARP) request to ensure that the LAN infrastructure is updated appropriately with the location of the active TN2602. Other devices within the LAN will update their old mapping in ARP cache with this new mapping.

Requirements for bearer duplication

The Communication Manager license file must have entries for each circuit pack, with the entries having identical voice channels enabled. In addition, both circuit packs must have the latest firmware that supports bearer duplication.

Duplicated TN2602AP circuit packs must be in the same subnet. In addition, the Ethernet switch or switches that the circuit packs connect to must also be in the same subnet. Ethernet switches can use signals from the TN2602AP firmware to identify the MAC address of the active circuit pack when they share subnets. This identification process provides a consistent virtual interface for calls.

Duplication and load balancing

A single port network can have up to two TN2602AP circuit packs only. As result, the port network can have either two duplicated TN2602AP circuit packs or two load balancing TN2602AP circuit packs, but not both a duplicated pair and a load-balancing pair. However, in a Communication Manager configuration, some port networks can have a duplicated pair of TN2602AP circuit packs and other port networks can have a load-balancing pair of TN2602AP circuit packs. Some port networks can also have single or no TN2602AP circuit packs.

Note:

If a pair of TN2602AP circuit packs previously used for load balancing are re-administered to be used for bearer duplication, only the voice channels of whichever circuit pack is active can be used. For example, If you have two TN2602 AP circuit packs in a load balancing configuration, each with 80 voice channels, and you re-administer the circuit packs to be in bearer duplication mode, you will have 80 (not 160) channels available. If you have two

TN2602 AP circuit packs in a load balancing configuration, each with 320 voice channels, and you re-administer the circuit packs to be in bearer duplication mode, you will have 320 (rather than 484) channels available.

TN2602AP IP Media Resource 320 features

The IP Media Resource 320 supports hairpin connections and the shuffling of calls between TDM connections and IP-to-IP direct connections. The IP Media Resource 320 can also perform the following functions:

- Echo cancellation
- Silence suppression
- Adaptive jitter buffer (320 ms)
- Dual-tone multifrequency (DTMF) detection
- AEA Version 2 and AES media encryption
- Conferencing
- QOS tagging mechanisms in layer 2 and 3 switching (Diff Serv Code Point [DSCP] and 802.1pQ layer 2 QoS)
- RSVP protocol

The TN2602AP IP Media Resource 320 circuit pack supports the following codecs for voice, conversion between codecs, and fax detection:

- G.711, A-law or Mu-law, 64 kbps
- G.726A-32 kbps
- G.729 A/AB, 8 kbps audio

The TN2602AP also supports transport of the following devices:

- Fax, Teletypewriter device (TTY), and modem calls using pass-through mode
- Fax, V.32 modem, and TTY calls using proprietary relay mode

Note:

V.32 modem relay is needed primarily for secure SCIP telephones (formerly known as Future Narrowband Digital Terminal (FNBDT) telephones) and STE BRI telephones.

- T.38 fax over the Internet, including endpoints connected to non-Avaya systems
- 64-kbps clear channel transport in support of firmware downloads, BRI secure telephones, and data appliances

Firmware download

The IP Media Resource 320 can serve as an FTP or SFTP server for firmware downloads to itself. However, this capability is activated by and available for authorized services personnel only.

As with the TN2302AP IP Media Processor, firmware upgrades of the TN2602AP circuit pack, are not call preserving. However, by using the **campon-busyout media-processor** command, a single or load-balanced TN2602AP circuit pack can be busied out without dropping calls, and then upgraded. In addition, with duplicated TN2602AP circuit packs, the standby TN2602AP circuit pack can be upgraded first, and then the circuit packs interchanged. The active circuit pack becomes the standby and can then be busied out and upgraded without dropping calls.

I/O adapter

The TN2602AP IP Media Resource 320 circuit pack has a services Ethernet port in the faceplate. The TN2602AP circuit pack also requires an input/output adapter that provides for one RS-232 serial port and two 10/100 Mbs Ethernet ports for LAN connections (though only the first Ethernet port is used). This Ethernet connection is made at the back of the IP Media Resource 320 slot.

Note:

The TN2302AP IP Media Processor on page 72 can also use this I/O adapter.

TN2312BP IP Server Interface (IPSI)

In configurations with the Duplex server controlling gateways, the bearer paths and the control paths are separate. Control information for port networks (PNs) travels over a LAN through the Ethernet switch. The control information terminates on the Duplex server at one end and on a TN2312BP IP Server Interface (IPSI) on the other end. Each IPSI can control up to five port networks by tunneling control messages over the Center-Stage or ATM network to PNs that do not have IPSIs.

Note:

IPSIs cannot be placed in a PN that has a Stratum-3 clock interface. Also, IPSIs cannot be placed in a remote PN that is using a DS1 converter.

In configurations that use a dedicated LAN for the control path, IPSI IP addresses are typically assigned automatically using DHCP service from the server. Also, a dedicated IPSI Ethernet connection to a laptop can be used to assign static IP addresses or for maintenance. In configurations using the customer's LAN, only static addressing is supported.

For information about installing and upgrading Duplex servers and IPSI configurations, see the *Avaya S8300, Simplex and Duplex server Library* CD, 555-233-825.

You can use the **status qos-parameters ipserver-interface** command to view the ISPI settings. The board location must be a valid TN2312 or TN8412 board location. For more information about the **status qos-parameters ipserver-interface** command, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 300431.

Detailed description

In Communication Manager Release 5.2, as an administrator, you can manage the following IPSI related parameters using a SAT interface or the System Management Interface:

- Set the values of QoS parameter fields (**DiffServ** and **802.1p**) on the System Parameters IP Server Interface screen. Default value for **DiffServ** is **46** and **802.1p** is **6**.
- Download QoS parameters to all IPSI boards. By default, **add ipserver-interface** or **change ipserver-interface** command pre-populates the QoS parameters if any IPSI boards are added.
- Set the values of Ethernet interface fields (**Auto**, **Speed**, or **Duplex**) on the IP Server Interface screen. **Speed** and **Duplex** fields display on the IP Server Interface screen, if **Auto** field is set to **n**.
- Changes to IPSI IP addresses (**IP Address**, **Subnet Mask, Gateway** address) on the IP Server Interface screen.

Note:

The initial IPSI IP address must be set manually by locally logging on to each IPSI board through a telnet or an ssh connection).

Firmware

The IPSI and the Communication Manager system use a capabilities exchange message to determine if an IPSI/SIPI board is capable of supporting the IPSI administration feature. IPSI firmware version 46 or greater and SIPI firmware version 16 or greater are required to support this capabilities exchange upon the port network coming into service.

IP Server Interface parameters

The IPSI sends QoS parameters, Ethernet settings, and IP address information to Communication Manager as specified in the *IP Server Interface parameters* table. The exchange of information is shared on socket creation.

Warning:

If the Ethernet interface settings (Auto, Speed, and Duplex) or the IPSI IP address settings (IP Address, Subnet Mask, and Gateway address) do not match with the network entity that the IPSI is communicating with, network communication can stop. To recover the settings you must go to the physical site of the IPSI, log in to the IPSI services port, and change the settings.

Table 7: IP Server Interface parameters

Description	Conditions/Comments	Required board is busied out
QoS parameters: On the System Management Interface, select **Installation** > **Configure Server**. Enable VLAN 802.1q priority tagging On the IP Server Interface screen Use System Level Parameter Values **802.1p** value **DiffServ** value		No
Ethernet interface settings: On the IP Server Interface screen Auto Speed Duplex	Reset the IPSI board for **Auto**, **Speed**, and **Duplex** values to take effect.	Yes
IP Address information: On the IP Server Interface screen IPSI **IP Address** Subnet Mask **Gateway** address	Reset the IPSI board for **IP Address**, **Subnet Mask**, and **Gateway** address values to take effect.	Yes

Communication Manager alarm on settings mismatch

Communication Manager compares its administered values on the SAT with the reported IPSI board values. The system generates a warning alarm if Communication Manager finds any discrepancies in the following values:

- **802.1p** value
- **DiffServ** value
- Ethernet **Auto** value

- Ethernet **Speed** value
- Ethernet **Duplex** value

You can view the alarm using the **display alarms** command or can enter an error type of **1** on the Display Errors screen.

Note:

Discrepancy between the SAT administration and the IPSI board values can happen if you have changed any of the IPSI board values using the CLI interface.

You can clear the alarm in one of the following ways:

- Set the correct values, and busyout or release the IPSI board.
- Change the values on the IP Server Interface screen and submit the screen.
- Change the values on the affected IPSI board using the CLI interface.

Default settings of IPSI QoS parameters

In the IPSI administration feature, QoS settings are standardized to communicate between the IPSI and Communication Manager. You can administer QoS parameters information on the Change IP Server Interface screen. The QoS default settings are shown in the following table:

Table 8: QoS default settings

Description	Defaults	Settings
Communication Manager to IPSI	**DiffServ** = **46**	**DiffServ** field on **change ipserver-interface** SAT screen.
	802.1p = **6**	**802.1p** field on **change ipserver-interface** SAT screen.
	802.1p/Q enabled = **no**	On the System Management Interface, select **Installation > Configure Server**. The system displays the Configure Server wizard. Click **Configure Interface**.
IPSI to Communication Manager	**DiffServ** = **46** (vintage >= 38) **DiffServ** = **40** (vintage < 38)	**DiffServ** field on **change ipserver-interface** SAT screen. Or, IPSI CLI interface
	802.1p = **6**	**802.1p** field on **change ipserver-interface** SAT screen. Or, IPSI CLI interface

	802.1p/Q enable d = **no**	IPSI CLI interface

Backward compatibility

The IPSI administration inter-operates with Communication Manager Release 5.0 or earlier by using the pre-existing QoS and administration interface. An IPSI uses the IPSI administration feature if IPSI firmware version is 46 or greater, SIPI firmware version is 16 or greater, and Communication Manager system supports Release 5.2 features.

The IPSI administration feature with Communication Manager Release 5.2 works with earlier IPSI boards as described in the following:

- Communication Manager assesses the administration capability of an IPSI board based on the capabilities exchange message.
- In general, if an older IPSI is unable to support this feature, then that IPSI needs to be administered using the CLI interface. If Communication Manager is not able to exchange the capabilities message with an older IPSI board, the following happens:
  - Communication Manager stops sending any IPSI QoS or Ethernet settings to the IPSI.
  - Communication Manager stops receiving the IPSI QoS or the Ethernet settings from IPSI.
  - The IPSI reports its status on the IP Server Interface screen.

MM760 VoIP Media Module

The Avaya MM760 Media Module is a clone of the motherboard VoIP engine.The MM760 provides the audio bearer channels for voice over IP calls, and is under control of the G700. Based on system administration of audio codecs, a MM760 can handle either 64 or 32 simultaneous channels of H.323 audio processing. If the IP Parameters screen specifies only G.711 mu-law or G.711 a-law as the audio codecs, the MM760 can service 64 channels. If any other codec type (G.723-5.3K, G.723-6.3K, or G.729) is administered, the MM760 can only service 32 channels. These call types can be mixed on the same resource. In other words, the simultaneous call capacity of the resource is 64 G.711 Equivalent Calls.

Note:

Customers who want an essentially non-blocking system must add an additional MM760 Media Module, if they use more than two MM710 Media Modules in a single chassis. The additional MM760 provides an additional 64 channels and is supported by only G700 Branch Gateway. The MM760 is not supported by G250, G350, G430 and G450 Branch Gateways.

MM760 Ethernet interface

The MM760 must have its own Ethernet address. The MM760 requires a 10/100 Base T Ethernet interface to support H.323 endpoints for Avaya IP trunks and stations from another G700 Branch Gateway. The MM760 is supported by only G700 Branch Gateway. The MM760 is not supported by G250, G350, G430 and G450 Branch Gateways.

Voice compression on the MM760

The MM760 supports on-board resources for compression and decompression of voice for G.711 (A- and μ-law), G.729 and 729B, and G.723 (5.3K and 6.3K). The VoIP engine supports the following functionality:

- RTP and RTCP interfaces
- Dynamic jitter buffers
- DTMF detection
- Hybrid echo cancellation
- Silence suppression
- Comfort noise generation
- Packet loss concealment

The MM760 also supports transport of the following:

- Teletypewriter device (TTY) tone relay over the Internet
- Faxes over a corporate IP intranet

Note:

The path between endpoints for FAX transmissions must use Avaya telecommunications and networking equipment.

Security alert:

Faxes sent to non-Avaya endpoints cannot be encrypted.

- Modem tones over a corporate IP intranet

Note:

The path between endpoints for modem tone transmissions must use Avaya telecommunications and networking equipment.

Avaya gateways

The following documents provide additional information about the administration of the Avaya gateways:

- *Administering Avaya Aura® Communication Manager*, (03-300509).
- *Upgrading, Migrating, and Converting Servers and Branch Gateways*, 03-300412.

IP trunks

The following sections describe the administration of IP trunks:

- SIP trunks on page 83
- H.323 trunks on page 85

SIP trunks

SIP is the Session Initiation Protocol, an endpoint-oriented messaging standard defined by the Internet Engineering Task Force (IETF). SIP “trunking” functionality is available on any of the Linux-based servers. These servers function as Plain Old Telephone Service (POTS) gateways, and they also support name/number delivery between and among the various non-SIP endpoints supported by Communication Manager (analog, DCP or H.323 stations and analog, digital or IP trunks), and SIP-enabled endpoints, such as the Avaya 4600-series SIP Telephones. In addition to its calling capabilities, IP Softphone R5 and later also includes optional instant-messaging client software, which is a SIP-enabled application, while continuing its full support of the existing H.323 standard for call control. Avaya SIP Softphone R2 and later releases fully support SIP for voice call control, as well as instant messaging and presence.

Communication Manager assigns two types of numbering to an incoming SIP trunk call:

- Private numbering: if the domain of the PAI, From, or Contact header in an incoming INVITE matches the authoritative domain of the called party network region.
- Public numbering: if the domain of the PAI, From, or Contact header in an incoming INVITE does not match the authoritative domain of the called party network region.

Public and private numbering plans are important when the incoming SIP trunk call is routed back over an ISDN trunk group.

ISDN defines numbering plans (NPI) and types of number (TON) within those plans. Following table lists the NPI and the values of TON within the plans:

Number Length	NPI=Public	NPI=Private	NPI=Unknown
Longest	TON=international	TON=Level 2	n/a
Middle	TON=national	TON=Level 1	n/a
Shortest	TON=Local	TON=Level 0	n/a
“don’t know”	TON=Unknown	TON=Unknown	TON=Unknown

If the caller does not know or does not want to specify the TON or NPI, it can set that value to ‘unknown’. When an incoming SIP call is routed to an ISDN network, Communication Manager always sets the TON to unknown.

Creating a SIP trunk signaling group

Procedure

1. Type `add signaling-group n`, where *n* is the signaling group number.

   The system displays the Signaling Group screen.
2. In the **Group Type** field, type `sip`.
3. In the **Near-end Node Name** field, type the node name of the procr.

   The node names are administered on the Node Names screen and the IP Interfaces screen.
4. In the **Far-end Node Name** field, type the far-end Session Manager name.

   Leave this field blank when the signaling group is associated with an unspecified destination.
5. In the **Near-end Listen Port** field, enter the port number depending on the transport method.

   For example, enter 5060 for TCP/UDP and 5061 for TLS.
6. In the **Far-end Listen Port** field, enter the number entered in the **Near-end Listen Port** field.
7. In the **Far-end Network Region** field, enter a value from 1 to 250 or leave the field blank.

   Identify the network assigned to the far end of the trunk group. The far end network region is used to obtain the codec set for negotiation of trunk bearer capability.
8. In the **Far-end Domain** field, type the name of the IP domain that is assigned to the far end of the signaling group.

For example, to route Session Manager calls within an enterprise, the domain assigned to the proxy server is used. For external SIP calling, the domain name can be the name of the SIP service provider.

Leave this field blank when you do not know the far-end domain.

9. In the **DTMF Over IP** field, specify the DTMF digits for transmission .

   The valid options for SIP signaling groups are:

   - **in-band**: All G711 and G729 calls pass DTMF in-band.
   - **out-of-band**: All IP calls pass DTMF out-of-band.
   - **rtp-payload**: This method is specified by RFC 2833. By default, RFC 2833 is the default value for newly added SIP signaling groups.

   For more information about the options, see *Avaya Aura® Communication Manager Screen Reference* .

10. Save the changes.
11. Type `add trunk-group n`, where *n* is the trunk group number.
12. In the **Group type** field, type `sip`.
13. In the **TAC** field, type the trunk access code number.
14. In the **Service type** field, type `tie`.
15. In the **Signaling Group** field, type the signaling group number that you configured earlier.
16. In the **Number of Members** field, type the number of members that you want to assign for the trunk.

    Enter a value in this field only when **member assignment** is auto.

17. Save the changes.

H.323 trunks

H.323 trunks use an ITU-T IP standard for LAN-based multimedia telephone systems. When IP-connected trunks are used, trunk groups can be defined as ISDN-PRI-equivalent tie lines between switches over an IP network.

The TN2302AP or TN2602AP enables H.323 trunk service using IP connectivity between an Avaya IP solution and another H.323 v2-compliant endpoint.

H.323 trunk groups can be configured as:

- Tie trunks supporting ISDN trunk features such as DCS+ and QSIG
- Generic tie-trunks permitting interconnection with other vendors' H.323 v2-compliant switches
- Direct-inward-dial (DID) type public trunks, providing access to the switch for unregistered users

Preparing to administer H.323 trunks

Procedure

1. Type **busy signaling-group number** to busy-out the signaling group.
2. Type **change signaling-group number**.
   The sytem displays the Signaling Group screen.
3. In the **Trunk Group for Channel Selection** field, type the trunk group number.
   If there is more than one trunk group assigned to this signaling group, the group entered in this field is the group that accepts incoming calls.
4. Save the changes.
5. Type **release signaling-group number** to release the signaling group.

Verifying customer options for H.323 trunking

About this task

Verify that H.323 trunking is set up correctly on the system-parameters customer-options screen. If any changes need to be made to fields on this screen, go to the Avaya Support website at http://support.avaya.com.

Procedure

1. Type **display system-parameters customer-options**.
2. Go to the Optional Features screen.
3. Verify that the following fields have been completed on pages 1 and 2 of this screen:
   - The value in the **G3 Version** field reflects the current version of Communication Manager.
   - The value in the **Maximum Administered H.323 Trunks** field is set to the number of trunks purchased. The value must be greater than 0.

This field is on page 2 of the screen.

- The **Maximum Administered Remote Office Trunks** field is set to the value to the number of office trunks purchased.

  This field is on page 2 of the screen.

4. Go to the page that displays the **IP trunks** and **ISDN-PRI** fields.
5. Verify that **IP Trunks** and **ISDN-PRI** are enabled.

   If not, obtain a new license file.

Administering C-LAN and IP Media Processor circuit packs (Simplex/Duplex Servers)

Procedure

1. Type **`add station next`**.

   The system displays the Station screen.
2. In the **Type** field, type the IP Telephone 4600-series model number, such as **4624**.

   The following phones are administered with an alias:

   - 4601 (administer as a 4602)
   - 4602SW (administer as a 4602)
   - 4690 (administer as a 4620)
3. In the **Port** field, type **x**, or **IP**.

   Note:

   A 4600-series IP Telephone is always administered as an X port, and then once it is successfully registered by the system, a virtual port number will be assigned. (Note that a station that is registered as unnamed is not associated with any logical extension or administered station record.)
4. For dual-connection architecture IP Telephones (R2 or earlier), complete the following fields:

   - In the **Media Complex Ext** field, type the H.323 administered extension.
   - In the **Port** field, type **x**.
5. Save the changes.

QoS parameters

Four parameters on the IP-Options System-Parameters screen determine threshold Quality of Service (QoS) values for network performance. You can use the default values for these parameters, or you can change them to fit the needs of your network. (See Setting network performance thresholds on page 174).

Administer additional QoS parameters, including defining IP Network Regions and specifying the codec type to be used. See Chapter 6: Voice and Network quality administration on page 143.

IP node names and IP addresses

Communication Manager uses node names to reference IP addresses throughout the system. Use the *IP Node Names* screen to assign node names and IP addresses to each node in the network with which this switch communicates through IP connections. The *Node Names* screen must be administered on each node in an IP network.

An IP node name can be any of these:

- Processor Ethernet (PE) IP Address
- C-LAN Ethernet or PPP IP Address
- Bridge or router IP Address
- CMS IP Address
- Communication Manager Messaging Address

Enter the AUDIX name and IP address on the *AUDIX Node Names* screen. Enter data for all other node types on the *IP Node Names* screen.

For H.323 connections, each MedPro Ethernet port (IP interface) on the local switch must also be assigned a node name and IP address on the *IP Node Names* screen.

Assign the node names and IP addresses in the network in a logical and consistent manner from the point of view of the whole network. Assign the names and addresses in the planning stages of the network and should be available from the the Avaya Support website at http://support.avaya.com.

Assigning IP Node Names

About this task

You must assigns node names and IP addresses to each node in the network. Administer the IP Node Names screen on each call server or switch in the network.

You should assign the node names and IP addresses logically and consistently across the entire network. These names and addresses should be assigned in the planning stages of the

network and should be available from the Avaya Support website at http://support.avaya.com.

Procedure

1. Type **change node-names ip**.
   The system displays the IP Node Names screen.
2. In the **Name** field, type the unique node names for the following:
   - Each C-LAN Ethernet port on the network
   - Each IP Media Processor
   - Each Remote Office
   - Other IP gateways and hops

   The default node name and IP address is used to set up a default gateway. This entry is automatically present on the Node Names screen and cannot be removed.

   When the Node Names screen is saved, the system automatically alphabetizes the entries by node name.
3. In the **IP Address** field, type the unique ip address for each node name.
4. Save the changes.

Defining IP interfaces (C-LAN, TN2302AP, or TN2602AP Load Balanced)

Procedure

1. Type **change ip-network-region**.
   The system displays the IP Network Region screen.
2. Complete the fields using the information in IP Network Region field descriptions on page 158.
3. Save the changes.

   Caution:

   If you change 802.1p/Q on the IP Network Region screen, it changes the format of the Ethernet frames. 802.1p/Q settings in Communication Manager must match those in all of the interfacing elements in your data network.

Defining IP interfaces (duplicated TN2602AP)

Procedure

1. Type **change ip-network-region**.
   The system displays the IP Network Region screen.
2. Complete the fields using the information in IP Network Region field descriptions on page 158.
3. Save the changes.

Caution:

If you change 802.1p/Q on the IP Network Region screen, it changes the format of the Ethernet frames. 802.1p/Q settings in Communication Manager must match those in all of the interfacing elements in your data network.

Assigning link through Ethernet data module

About this task

Note:

The S8300D Server does not support data modules.

This section describes how to administer an Ethernet data module for the connection between the C-LAN circuit pack's Ethernet port (port 17) and the LAN. The data module associates a link number and extension number with the C-LAN Ethernet port location. This association is used by the processor to set up and maintain signaling connections for multimedia call handling.

The C-LAN Ethernet port is indirectly associated with the C-LAN IP address through the slot location (which is part of the port location) on the IP Interfaces screen and the node name, which is on both the **IP Interfaces** and Node Names screens.

Procedure

1. Type **add data-module next**.
   The system displays the Data Module screen.
2. In the **Data Extension** field, Communication Manager automatically sets the value with the **next** qualifier or type the extension number.
3. In the **Type** field, type **Ethernet**.
   This indicates the data-module type for this link.

4. In the **Port** field, set the ethernet connections to port **17** on the C-LAN circuit pack.
5. In the **Link** field, type the link number, a link not previously assigned on this switch.
6. In the **Name** field, the name displays in lists generated by the **`list data module`** command.
7. In the **Network uses 1's for broadcast addresses** field, type **y** if the private network contains only Avaya switches and adjuncts.

   Type **n** if the network includes non-Avaya switches that use the 0's method of forming broadcast addresses.

   For more information on the fields that can display on this screen, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.
8. Submit the screen.

Best Service Routing (optional)

Use H.323 trunks to implement Best Service Routing (BSR). You can use H.323 trunks for polling, or for both polling and interflow. Because polling requires only a small amount of data exchange, the additional network traffic is insignificant. However, interflow requires a significant amount of bandwidth to carry the voice data. Depending on the other uses of the LAN/WAN and its overall utilization rate, voice quality could be degraded to unacceptable levels.

Avaya recommends that if H.323 trunks are used for BSR interflow, the traffic should be routed to a low-occupancy or unshared LAN/WAN segment. Alternatively, you might want to route internal interflow traffic, which have lower quality-of-service requirements, over H.323 trunks, and route customer interflow traffic over circuit-switched tie trunks.

Administering H.323 trunk

Procedure

1. Create one or more IP Codec sets that enable the appropriate transmission modes for the endpoints on your gateways.

   See IP CODEC sets on page 153.

Note:

You create the FAX, modem, TTY, and clear channel settings (including redundancy) on the second page of the IP Codec Set screen.

2. Assign each codec set to the appropriate network region.

   See IP network regions on page 156.

3. Assign the network region to the appropriate device(s):

   - TN2302AP or TN2602AP (see Defining IP interfaces (C-LAN, TN2302AP, or TN2602AP Load Balanced) on page 89)
   - Avaya G250, G350, G430, G450, or G700 Branch Gateway

4. If the TN2302AP or TN2602AP resources are shared among administered network regions, administer inter-network region connections.

   See Manually interconnecting the network regions on page 168.

H323 trunk signaling group

Create a signaling group that is associated with H.323 trunks that connect this switch to a far-end switch. One or more unique signaling groups must be established for each far-end node to which this switch is connected through H.323 trunks.

Note:

The following steps address only those fields that are specifically related to H.323 trunks. The other fields are described in *Administering Avaya Aura® Communication Manager*, 03-300509.

Creating an H.323 trunk signaling group

Procedure

1. Type **`add signaling-group number`**.

   The system displays the Signaling Group screen.

2. In the **Group Type** field, type **h.323**.

3. In the **Trunk Group for Channel Selection** field, leave the field blank until you create a trunk group in the following task, then use the change command and enter the trunk group number in this field.

4. In the **T303 Timer** field, type the number of seconds the system waits for a response from the far end before invoking Look Ahead Routing.

The system displays this field only when the Group Type field is isdn-pri (DS1 Circuit Pack screen) or h.323 (Signaling Group screen).

5. In the **H.245 DTMF Signal Tone Duration (msec)** field, specify the tone duration of DTMF tones sent in H.245-signal message when **DTMF over IP**: field is set to **out-of-band** on the **Signaling Group screen** for IP Trunks.

   The value of this field can be either in the range 80 ms to 350 ms or blank. The default value is blank.

6. In the **Near-end Node Name** field, type the node name for the C-LAN IP interface on this switch.

   The node name must be administered on the Node Names screen and the IP Interfaces screen.

7. In the **Far-end Node Name** field, type the node name for the far-end C-LAN IP Interface used for trunks assigned to this signaling group.

   The node name must be administered on the Node Names screen on this switch.

   Leave blank when the signaling group is associated with an unspecified destination.

8. In the **Near-end Listen Port** field, enter an unused port number from the range **1719**, **1720** or **5000–9999**.

   Avaya recommends **1720**. If the **LRQ** field is **y**, enter `1719`.

9. In the Far-end Listen Port field, enter the same number as the one in the **Near-end Listen Port** field.

   This number must match the number entered in the **Near-end Listen Port** field on the Signaling Group screen for the far-end switch.

   Leave blank when the signaling group is associated with an unspecified destination.

10. In the **Far-end Network Region** field, enter a value between **1-250** or leave the field blank to select the region of the near-end node (C-LAN).

    Identify network assigned to the far end of the trunk group. The region is used to obtain the codec set used for negotiation of trunk bearer capability. If specified, this region is used instead of the default region (obtained from the C-LAN used by the signaling group) for selection of a codec.

11. In the LRQ Required field, type **n** when the far-end switch is an Avaya product and H.235 Annex H Required? is set to **n**.

    Type **y** when:

    - 235 Annex H Required? is set to **y**, or
    - the far-end switch requires a location request to obtain a signaling address in its signaling protocol.

12. In the **Calls Share IP Signaling Connection** field, type **y** for connections between Avaya equipment.

Type **n** when the local and/or remote switch is not Avaya switch.

13. In the **RRQ Required** field, type **y** when a vendor registration request is required.
14. In the **Bypass if IP Threshold Exceeded** field, type **y** to automatically remove from service trunks assigned to this signaling group when IP transport performance falls below limits administered on the Maintenance-Related System Parameters screen.
15. In the **H.235 Annex H Required** field, type **y** to indicate that the Avaya Aura® CM server requires the use of H.235 amendment 1 with annex H protocol for authentication during registration.
16. In the **DTMF Over IP** field, specify the transmission of the DTMF digits.

    The valid options for SIP signaling groups are:in-band and rtp-payload.

    The valid options for H.323 signaling groups are: in-band, in-band-g711, out-of-band, and rtp-payload.
17. In the **Direct IP-IP Audio Connections** field, type **y** to save on bandwidth resources and improve sound quality of voice over IP (VoIP) transmissions.

    Direct audio connections between H.323 endpoints. For SIP Enablement Services (SES) trunk groups, this value helps in direct audio connections between SES endpoints.
18. In the **Link Loss Delay Timer** field, specify how long to hold the call state information in the event of an IP network failure or disruption.

    Communication Manager preserves calls and starts this timer at the onset of network disruption (signaling socket failure). If the signaling channel recovers before the timer expires, all call state information is preserved and the signaling channel is recovered. If the signaling channel does not recover before the timer expires, the system:

    - raises an alarm against the signaling channel
    - maintains all connections with the signaling channel
    - discards all call state information about the signaling channel
19. In the **IP Audio Hairpinning** field, type **y** to enable hairpinning for H.323 or SIP trunk groups.

    Using the **IP Audio Hairpinning** field entry, you have the option for H.323 and SIP Enablement Services (SES)-enabled endpoints to be connected through the IP circuit pack in the server or switch, without going through the time division multiplexing (TDM) bus.
20. In the **Interworking Message** field, select a value that determines what message Communication Manager sends when an incoming ISDN trunk call interworks (is routed over a non-ISDN trunk group).

Normally select the value, **PROGress**, which asks the public network to cut through the B-channel and let the caller hear tones such as ringback or busy tone provided over the non-ISDN trunk.

Selecting the value **ALERTing** causes the public network in many countries to play ringback tone to the caller. Select this value only if the DS1 is connected to the public network, and it is determined that callers hear silence (rather than ringback or busy tone) when a call incoming over the DS1 interworks to a non-ISDN trunk.

21. In the DCP/Analog Bearer Capability field, set the information transfer capability in a bearer capability IE of a setup message to **speech** or **3.1kHz**.

    3.1kHz is a default value. The default value provides 3.1kHz audio encoding in the information transfer capability. Selecting the value of **speech** provides speech encoding in the information transfer capability.

22. If using DCS, go to the Administered NCA TSC Assignment page of this screen.

    Enter NCA TSC information on this screen according the detailed descriptions in the *Screen Reference Avaya Aura® Communication Manager Screen Reference*, 03-602878.

23. Save the changes.

Creating a trunk group for H.323 trunks

About this task

This task creates a new trunk group for H.323 trunks. Each H.323 trunk must be a member of an ISDN trunk group and must be associated with an H.323 signaling group.

Note:

The following steps address only those fields that are specifically related to H.323 trunks. The other fields are described in the *Administering Avaya Aura® Communication Manager*, 03-300509

Procedure

1. Type **`add trunk-groupnext`**.

   The system displays the Trunk Group screen.

2. In the **Group Type** field, type **isdn**.
3. In the **Carrier Medium** field, type **H.323**.
4. In the **Service Type** field, type **tie**.
5. In the **TestCall ITC** field, type **unre** (unrestricted).

6. In the **TestCall BCC** field, type **0**.
7. In the **Codeset to Send Display** field, type **0**.

   Note:

   The Outgoing Display field might need to be changed if the far-end is not Avaya's.
8. Go to the Trunk Features page of this screen.
9. In the **Send Name** field, the **Send Calling Number** field, and the **Send Connected Number** field, check the value entered.

   If **y** is entered, either the ISDN Numbering - Public/Unknown Format screen, or the ISDN Numbering - Private screen (based on the **Format** field) is accessed to construct the actual number to be sent to the far end.
10. To add a second signaling group, go to the Group Member Assignments page of this screen.

    Note:

    Each signaling group can support up to 31 trunks. If you need more than 31 trunks between the same two switches, add a second signaling group with different listen ports and add the trunks to the existing or second trunk group.
11. In the **Port** field, type **ip**.

    When the screen is submitted, this value is automatically changed to a **T** number (**Txxxxx**).
12. In the **Name** field, type a 10-character name to identify the trunk.
13. In the **Sig Grp** field, type the number for the signaling group associated with this H.323 trunk.

Modifying the H.323 trunk signaling group

About this task

Modify the Signaling Group screen to add a trunk group number to the **Trunk Group for Channel Selection** field.

Procedure

1. Type **`busy signaling-group number`** to busy-out the signaling group.
2. Type **`change signaling-group number`**.

   The sytem displays the Signaling Group screen.

3. In the **Trunk Group for Channel Selection** field, type the trunk group number.
   If there is more than one trunk group assigned to this signaling group, the group entered in this field is the group that accepts incoming calls.
4. Save the changes.
5. Type **`release signaling-group number`** to release the signaling group.

Dynamic generation of private/public calling party numbers

Often it is necessary to generate a private Calling Party Number (CPN) for calls within a network, but a public CPN for calls that route through the main network switch to the PSTN.

See the following network:

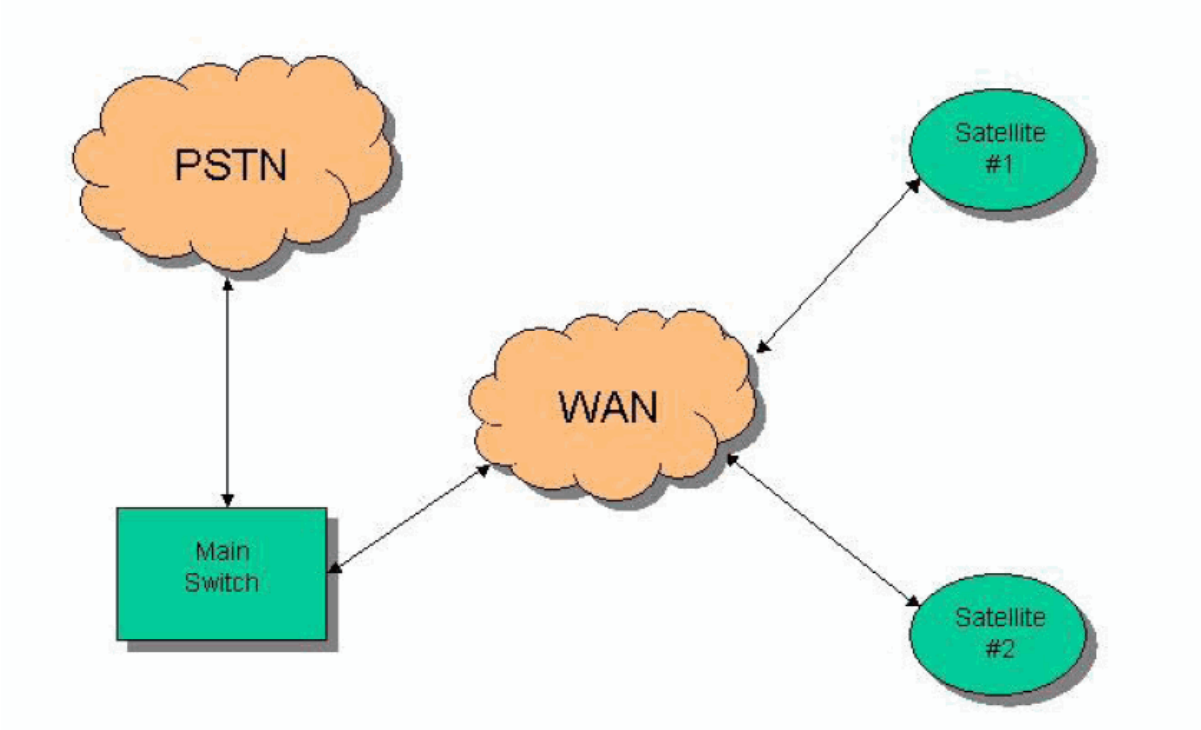


Figure 10: Private/public calling party numbers (CPN)

In this network, the customer wants to use internal numbering among the nodes of the network (for example, a 4-digit Uniform Dial Plan (UDP)), but when any node dials the PSTN, to route the call to the PSTN through the main switch.

On page 2 of the ISDN Trunk Group screen, set the **Numbering Format** field to **private** or **unk-pvt**. (The value **unk-pvt** means “encode the number as an” unknown" type of number, but use the Numbering-Private Format screen to generate the actual number.)

Note:

IP trunks function as ISDN trunks in this respect.

In the network example, the system only generates a Private CPN if the caller dials a Private (level 0/1/2) or Unknown (unk-unk) number. If the caller dials a Public number, the system generates a Public CPN. It is necessary to fill out the **Numbering-Private Format** and **Numbering-Public/Unknown Format** forms appropriately, and then to set the IP trunk groups on the two satellites to use **private** or **unk-pvt Numbering Format** for their CPNs.

Note:

You can designate the type of number for an outgoing call as Private (level 0/1/2) either on the AAR Analysis screen or on the Route Pattern screen, but you can only designate the type of number as Unknown (**unk-unk**) on the Route Pattern screen. If you are using UDP, then the Type of Number you should use is Unknown.

The default **Call Type** on the AAR Analysis screen is **aar**. For historical reasons, **aar** maps to a “public” numbering format. Therefore, you must change the **Call Type** for calls within your network from **aar** to a **private** or **unk-unk** type of number. For a UDP environment, the recommended way is to set the **Numbering Format** to **unk-unk** on the Route Pattern screen.

Avaya Phones

The following sections describe the installation and administration of Avaya IP telephones:

- IP Softphones on page 98
- Avaya IP telephones on page 102

IP Softphones

IP Softphones operate on a personal computer equipped with Microsoft Windows and with TCP/IP connectivity through Communication Manager. Avaya offers the following Softphone applications:

- IP Softphone for any telephone user
- IP Agent for call center agents
- Softconsole for console attendants
- One-X Communicator
- SIP softphone
- one-X Portal as software-only telephone

IP Softphones can be configured to operate in any of the following modes:

- Road-warrior mode consists of a personal computer running the Avaya IP Softphone application and Avaya iClarity IP Audio, with a single IP connection to an Avaya server or gateway.
- Telecommuter mode consists of a personal computer running the Avaya IP Softphone application with an IP connection to the server, and a standard telephone with a separate PSTN connection to the server.
- Shared Control mode provides a registration endpoint configuration using which an IP Softphone and a non-Softphone telephone can be in service on the same extension at the same time. In this new configuration, the call control is provided by both the Softphone and the telephone endpoint. The audio is provided by the telephone endpoint.

Documentation on how to set up and use the IP Softphones is included on the CD-ROM containing the IP Softphone software. Procedures for administering Communication Manager to support IP Softphones are given in *Administering Avaya Aura® Communication Manager,03-300509*.

This section focuses on administration for the trunk side of the Avaya IP Solutions offer, plus a checklist of IP Softphone administration. Comprehensive information on the administration of IP Softphones is given in *Administering Avaya Aura® Communication Manager*, 03-300509.

There are two main types of IP Softphone configurations:

- Administering a Telecommuter Telephone on page 99
- Administering a Road-warrior telephone on page 101

Communication Manager can distinguish between various IP stations at RAS using the product ID and release number sent during registration. An IP telephone with an Avaya manufacturer ID can register if the number of stations with the same product ID and the same or lower release number *is less than* the administered system capacity limits. System limits are based on the number of simultaneous registrations. Note that a license is required for each station that is to be IP softphone enabled.

Administering a Telecommuter Telephone

About this task

The Telecommuter uses two connections, one to the personal computer over the IP network and another connection to the telephone over the PSTN. IP Softphone personal computer software handles the call signaling. With IP Softphone R5 or greater, iClarity is automatically installed to handle voice communications.

Note:

The System Parameters Customer Options screen is display only. Use the **`display system-parameters customer-options`** command to review the screen. The License File controls the system software release, the Offer Category, features, and capacities. The

init login does not have the ability to change the customer options, offer options, or special applications screens.

Procedure

1. Type **`display system-parameters customer-options`** and press `Enter`.

   The system displays the System Parameters Customer Options screen.

2. Verify that IP Softphone is enabled.

   Review the following fields on the screen:

   - In the **Maximum Concurrently Registered IP Stations** field, the value must be greater than **0**, and must be less than or equal to the value for Maximum Ports.

     This field identifies the maximum number of IP stations that are simultaneously registered, not the maximum number that are simultaneously administered.

   - In the **Maximum Concurrently Registered Remote Office Stations** field, the value must be greater than **0**, and must be less than or equal to the value for Maximum Ports.

     This field specifies the maximum number of remote office stations that are simultaneously registered, not the maximum number that are simultaneously administered.

   - In the **IP Stations** field, the value should be **y**.
   - In the **Product ID** field, for new installations, IP Soft, IP Telephone, IP Agent and IP ROMax, the system displays the product IDs automatically.

     This is a 10-character field with any character string.

   - In the **Rel. (Release)** field, check the the release number.
   - In the **Limit** field, check the value.

     This field defaults to the maximum value, based on the **Concurrently Registered Remote Office Stations** field on page 1 of the ***System Parameters Customer Options*** screen.

3. Type **`add station next`** and press `Enter`.

   The system displays the Station screen.

4. Add a DCP station (or change an existing DCP station).

5. In the **Type** field, type the telephone model, such as **6408D**.

6. In the **Port** field, type **x** if virtual, or the port number of an existing telephone.

7. In the **Security Code** field, type the station security code that is assigned to the extension as a password.

8. In the **IP Softphone** field, type **y**.

9. Go to page 2; verify whether the field **Service Link Mode**: *as-needed* is set as shown.
10. Install the IP Softphone software on the user's personal computer.

Administering a Road-warrior telephone

About this task

The sofphone application runs on a personal computer that is connected over an IP network. In road-warrior mode, the application uses two channels: one for call control signaling and one for voice.

Note:

The System Parameters Customer Options screen is display only. Use the **display system-parameters customer-options** command to review the screen. The License File controls the system software release, the Offer Category, features, and capacities. The *init* login does not have the ability to change the customer options, offer options, or special applications screens.

Procedure

1. Type **display system-parameters customer-options**.
2. Verify that IP Softphone is enabled.

   Go to the appropriate pages on the System Parameters Customer Options screen to review the following fields:

   - In the Maximum Concurrently Registered IP Stations field, the value must be greater than **0**.
   - In the **IP Stations** field, the value must be **y**.
   - In the **Product ID** field, for new installations, IP Soft, IP Telephone, IP Agent and IP ROMax, the system displays the product IDs automatically.

     This is a 10-character field with any character string.
   - In the **Rel. (Release)** field, check the release number.
   - In the Limit field, check the default value.

     The default value is **1**.
3. Type **add station next** and press Enter.

   The system displays the Station screen.
4. Add a DCP station (or change an existing DCP station).
5. In the **Type** field, type the telephone model to use, such as **6408D**.

6. In the Port field, type **x** if virtual, or the port number of an existing telephone.
   If only an IP Softphone, type **IP**.
7. In the **Security Code** field, type the station security code that is assigned to the extension as a password.
8. In the **IP Softphone** field, type **y**.
9. Go to page 2; **Service Link Mode**: `as-needed`.
   Install the IP Softphone software on the user's personal computer (iClarity automatically installed with the IP Softphone R2 or greater).

Avaya IP telephones

The Avaya line of digital business telephones uses Internet Protocol (IP) technology with Ethernet line interfaces and has downloadable firmware.

IP Telephones provide support for dynamic host configuration protocol (DHCP) and either Trivial File Transfer Protocol (TFTP) or Hypertext Transfer Protocol (HTTP) over IPv4/UDP, which enhance the administration and servicing of the telephones.

For information on feature functionality of the IP telephones, see the *Avaya Aura® Communication Manager Hardware Description and Reference* (555-245-207), or the appropriate IP Telephone user's guides.

For more information on installing and administering Avaya IP telephones, see

- *4600 Series IP Telephone Installation Guide*, 555-233-128
- *4600 Series IP Telephone LAN Administrator's Guide*, 555-233-507
- *Avaya one-X Deskphone Edition 9600 Series IP Telephone Installation and Maintenance Guide, 16-300694*
- *Avaya one-X Deskphone Edition 9600 Series IP Telephones Administrator Guide*, 16-300698
- *Avaya one-X Deskphone Value Edition 1600 Series IP Telephones Installation and Maintenance Guide*, 16-601438
- *Avaya one-X Deskphone Value Edition 1600 Series IP Telephones Administrator Guide Release 1.0*, 16-601443

For more information on IP Wireless Telephone Solutions, visit http://support.avaya.com

4600-series IP telephones

The 4600-series IP Telephone product line possesses a number of shared model features and capabilities. All models also feature

- Downloadable firmware
- Automatic IP address resolution through DHCP
- Manual IP address programming.

The 4600-series IP Telephone product line includes the following telephones:

- Avaya 4601 IP telephone
- Avaya 4602 and 4602SW IP telephone
- Avaya 4610SW IP telephone
- Avaya 4620 and 4620SW IP telephone
- Avaya 4622SW IP telephone
- Avaya 4622 IP telephone
- Avaya 4625 IP telephone
- Avaya 4630SW IP Screenphone
- Avaya 4690 IP conference telephone

Support for SIP-enabled applications can be added to several of these IP telephones via a model-specific firmware update. See the Avaya Firmware Download website for more details.

96x1-series IP telephones

The 96x1-series IP Telephone product line possesses a number of shared model features and capabilities. All models also feature:

- Downloadable firmware
- Automatic IP address resolution through DHCP
- Manual IP address programming.

The 96x1-series IP Telephone product line includes the following telephones:

- Avaya 9611 H.323 and SIP deskphones for everyday users
- Avaya 9621 H.323 and SIP deskphones for essential users
- Avaya 9641 H.323 and SIP deskphones for essential users
- Avaya 9610 IP telephone for Walkup users

9600-series IP telephones

The 9600-series IP Telephone product line possesses a number of shared model features and capabilities. All models also feature:

- Downloadable firmware
- Automatic IP address resolution through DHCP
- Manual IP address programming.

The 9600-series IP Telephone product line includes the following telephones:

- Avaya 9610 IP telephone for Walkup users
- Avaya 9620 IP telephone for the Everyday user
- Avaya 9630 IP telephone with advanced communications capabilities
- Avaya 9640 IP telephone with advanced communications capabilities, color display
- Avaya 9650 IP telephone for the executive administrative assistant

Support for SIP-enabled applications can be added to several of these IP telephones via a model-specific firmware update. See the Avaya Firmware Download website for more details.

1600-series IP telephones

The 1600-series IP Telephone product line possesses a number of shared model features and capabilities. All models also feature:

- Downloadable firmware
- Automatic IP address resolution through DHCP
- Manual IP address programming.

The 4600-series IP Telephone product line includes the following telephones:

- Avaya 1603 IP telephone for Walkup users
- Avaya 1608 IP telephone for the Everyday user
- Avaya 1616 IP telephone for the Navigator user

Support for SIP-enabled applications can be added to several of these IP telephones via a model-specific firmware update. See the Avaya Firmware Download website for more details.

IP telephone hardware and software

IP Telephones are shipped from the factory with operational firmware installed. Some system-specific software applications are downloaded from a TFTP or HTTP server through automatic

power-up or reset. The IP Telephones search and download new firmware from the file server before attempting to register with Communication Manager.

During a Communication Manager upgrade, any data in the /tftpboot directory is overwritten with new software and firmware. For more detailed information on managing the firmware and configuration files for the 4600-series IP telephones during Communication Manager upgrades, see *Installing and Upgrading the Avaya G700 Branch Gateway and Avaya S8300 Server* (555-234-100), or *Upgrading, Migrating, and Converting Servers and Gateways* (03-300412).

The software treats the 4600-series and 9600-series IP Telephones as any new station type, including the capability to **`list/display/change/duplicate/remove station`**.

Note:

Audio capability for the IP telephones requires the presence of TN2302AP IP Media Processor or TN2602AP Media Resource 320 circuit pack, either of which provide hairpinning and IP-IP direct connections. Using a media processor resource conserves TDM bus and timeslot resources and improves voice quality.

Note:

The 4600-series IP telephone also requires a TN799DP Control-LAN (C-LAN) circuit pack for the signaling capability on the DEFINITY Server csi platform. You do not need a C-LAN circuit pack to connect an IP Telephone if your system has built-in (for example, using an Avaya S8300D Server or Avaya Duplex server) or Processor Ethernet capability.

Note:

To register H.323 endpoints that do not use TTS, one of the connected network regions of the IP station must have a PROCR or a CLAN.

Installing TN2302AP, TN2602AP, and TN799DP circuit packs

Procedure

1. Determine the carrier/slot assignments of the circuit packs to be added.
2. Insert the circuit pack into the slot specified in step 1.

   Note:

   You do not have to switch off the cabinet to install the circuit packs.

Administering Avaya IP telephones

About this task

IP Telephones R1.5 or greater use a single connection, and you only need to administer the station type.

Procedure

1. Type **add station next**.

   The system displays the Station screen.

2. In the **Type** field, type the IP Telephone 4600-series model number, such as **4624**.

   The following phones are administered with an alias:

   - 4601 (administer as a 4602)
   - 4602SW (administer as a 4602)
   - 4690 (administer as a 4620)

3. In the **Port** field, type **x**, or **IP**.

   Note:

   A 4600-series IP Telephone is always administered as an X port, and then once it is successfully registered by the system, a virtual port number will be assigned. (Note that a station that is registered as unnamed is not associated with any logical extension or administered station record.)

4. For dual-connection architecture IP Telephones (R2 or earlier), complete the following fields:

   - In the **Media Complex Ext** field, type the H.323 administered extension.
   - In the **Port** field, type **x**.

5. Save the changes.

Hairpinning, shuffling, and Direct Media

Communication Manager can shuffle or hairpin call path connections between two IP endpoints by rerouting the voice channel away from the usual TDM bus connection and creating a direct IP-to-IP connection. Shuffling and hairpinning are similar because they preserve connection and conversion resources that might not be needed, depending on the compatibility of the endpoints that are attempting to interconnect.

Shuffling and hairpinning techniques differ in the way that they bypass the unnecessary call-path resources.

Shuffled or hairpinned connections:

- Conserve channels on the TN2302AP IP Media Processor and TN2602AP IP Media Resource 320.
- Bypass the TDM bus, conserving timeslots.
- Improve voice quality by bypassing the codec on the TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit packs.

Because shuffling frees up more resources on the TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit packs than hairpinning does, Communication Manager first checks both endpoints to determine whether Communication Manager uses the criteria to determine whether a shuffled audio connection is possible. If the shuffling criteria are not met, Communication Manager routes the call according to the criteria for hairpinning, if hairpinning is enabled. If hairpinning is not enabled, Communication Manager routes the call to the TDM bus. Both endpoints must connect through the same TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 for Communication Manager to shuffle or hairpin the audio connection.

For information on interdependencies that enable hairpinning and shuffling audio connections, see *Hairpinning and shuffling administration interdependencies*. For Network Address Translation (NAT), see *Network Address Translation*.

Hardware and endpoints

The TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 circuit pack is required for shuffling or hairpinning audio connections.

The specific endpoint types that you can administer for hairpinning or shuffling are:

- All Avaya IP stations
- Other vendors' H.323-compatible stations

Shuffled audio connections

Shuffling an audio connection between two IP endpoints means rerouting voice channel away from the usual TDM bus connection and creating a direct IP-to-IP connection. Shuffling saves such resources as TN2302AP or TN2602AP channels and TDM bus time slots and improves voice quality because the shuffled connection bypasses the TN2302AP's or TN2602AP's codec. Both endpoints must be capable of shuffling (support H.245 protocol) before Communication Manager can shuffle a call.

Communication Manager uses the following criteria to determine whether a shuffled audio connection is possible:

- A point-to-point voice connection exists between two endpoints.
- No other active call (in-use or held) that requires TDM connectivity (for example, applying tones, announcement, conferencing, and others) exists on either endpoint.
- The endpoints are in the same network region or in different, interconnected regions.
- Both endpoints or connection segments are administered for shuffling by setting the **Direct IP-IP Audio Connections** field to `y` for shuffled IP calls to use a public IP address (default).
- If the **Direct IP-IP Audio Connections** field is `y` (yes), but during registration the endpoint indicates that it does not support audio shuffling, then a call cannot be shuffled. If the **Direct IP-IP Audio Connections** field is `n` (no), but during registration the endpoint indicates that it can support audio shuffling, then calls to that endpoint cannot be shuffled, giving precedence to the endpoint administration.
- The rules for Inter-network region connection management on page 121 are met.
- There is at least one common codec between the endpoints involved and the Inter-network region Connection Management codec list.
- The endpoints have at least one codec in common as shown in their current codec negotiations between the endpoint and the switch.
- Both endpoints can connect through the same TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 circuit packs.

Examples of shuffling

Shuffling within the same network region

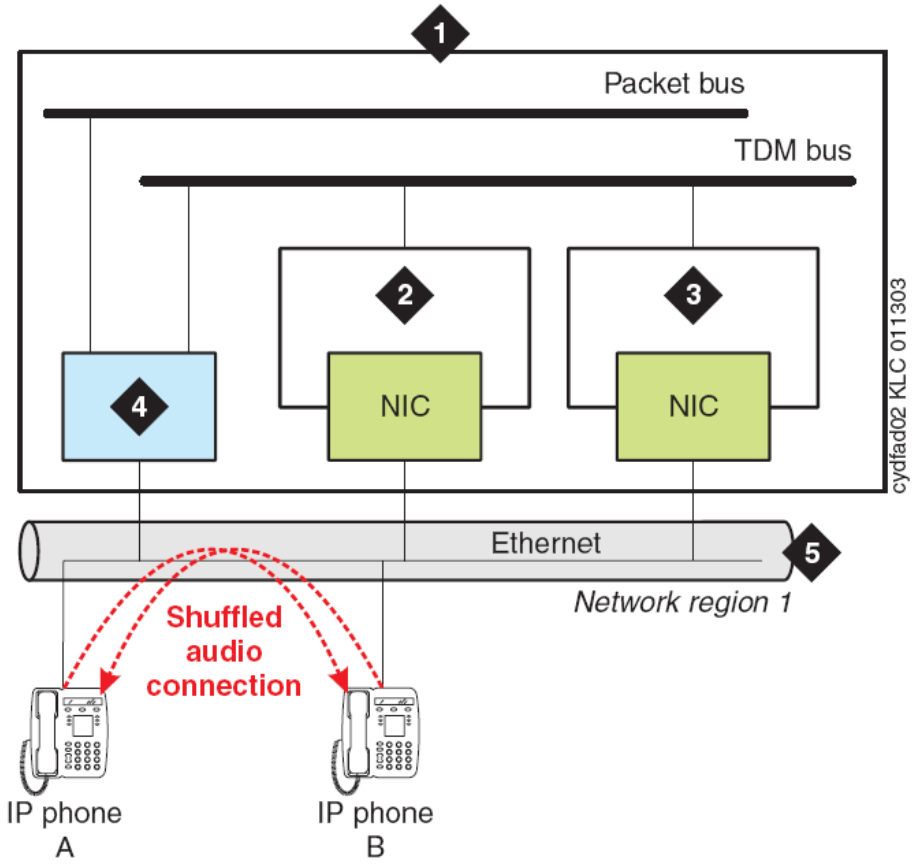


Figure 11: Shuffled audio connection between IP endpoints in the same network region

Number	Description
1	Avaya server
2	TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit pack
3	TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit pack
4	TN799 Control LAN (C-LAN) circuit pack
5	LAN/WAN segment administered in Communication Manager as network region 1.

The *Shuffled audio connection between IP endpoints in the same network region* figure, is a schematic of a shuffled connection between two IP endpoints within the same network region. After the call is shuffled, the IP Media Processors are out of the audio connection, and those channels are free to serve other media connections.

Shuffling between different network regions

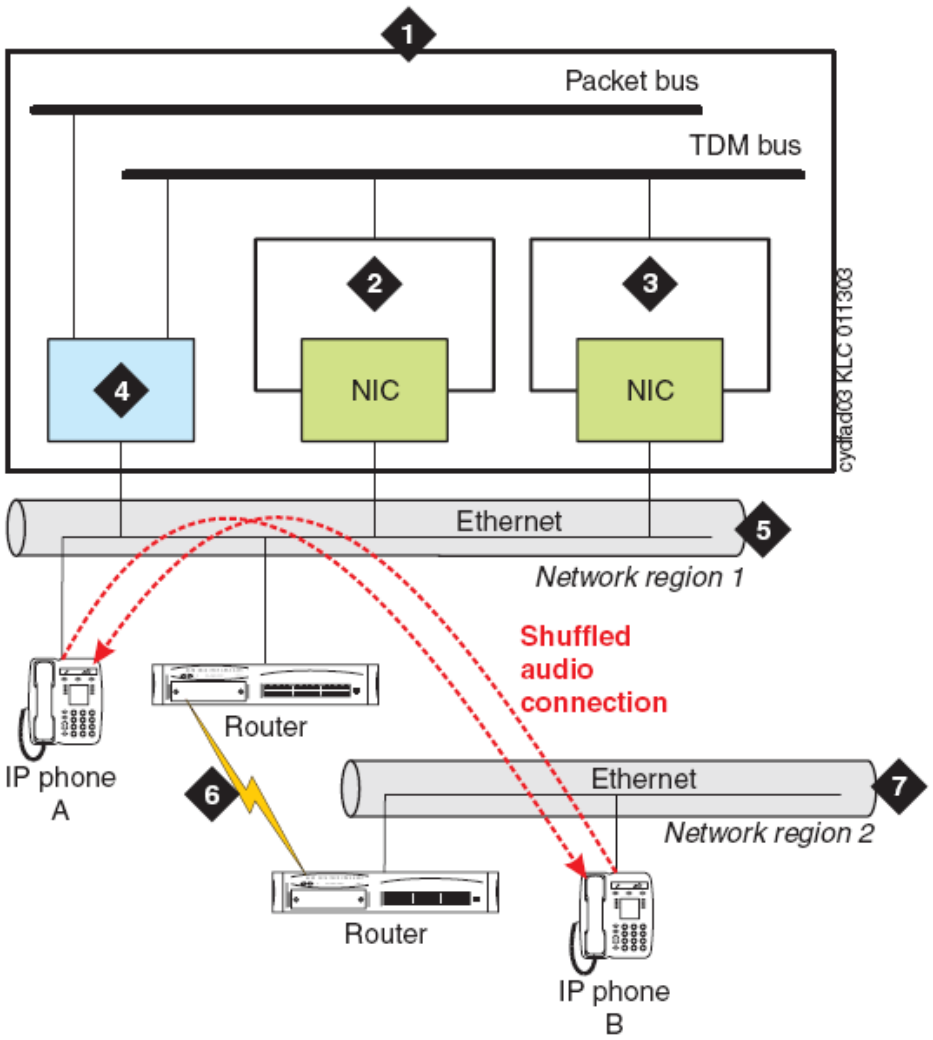


Figure 12: Shuffled audio connection between IP endpoints in different network regions

Number	Description
1	Avaya server
2	TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit pack

Number	Description
3	TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit pack
4	TN799 Control LAN (C-LAN) circuit pack
5	LAN/WAN segment administered in Communication Manager as network region 1.
6	IP voice packet path between LAN routers
7	LAN/WAN segment administered in Communication Manager as network region 2.

The *Shuffled audio connection between IP endpoints in different network regions* figure is a schematic of a shuffled audio connection between two IP endpoints that are in different network regions that are interconnected and the inter-network region connection management rules are met. After the call is shuffled, both Media Processors are bypassed, making those resources available to serve other media connections. The voice packets from IP endpoints flow directly between LAN routers.

Determining whether an endpoint supports shuffling

About this task

Placing a test call from an endpoint that is capable of shuffling to another endpoint whose shuffling capability is unknown can help you to determine whether an endpoint supports audio shuffling or not.

Procedure

1. Administer the **Direct IP-IP Audio Connections** field on page 2 as **y** (yes) on both endpoint's station screen (**`change station extension`**).
2. From the endpoint that can support shuffling, place a call to the endpoint that you are testing.

   Wait 2 minutes.
3. At the SAT type **`status station extension`** (administered extension of the endpoint that you are testing) and press `Enter`to display the Station screen for this extension.
4. Note the **Port** field value in the **GENERAL STATUS** section of page 1.
5. Scroll to page 4

In the **AUDIO CHANNEL** section note the value of the **Audio** field under the **Switch Port** column.

- If the values are the same, the endpoint is capable of shuffling.

  Administer the **Direct IP-IP Audio Connections** field (**`change station extension`**, page 2) as **y** (yes).

- If the values are different, then the endpoint cannot shuffle calls.

  Administer the **Direct IP-IP Audio Connections** field (**`change station extension`**, page 2) as **n** (no).

Administrable loss plan

To prevent audio levels from changing when a 2-party call changes from the TDM bus to a shuffled or hairpinned connection, two party connections between IP endpoints are not subject to the switch's administrable loss plan. Although IP endpoints can be assigned to administrable loss groups, the switch is only able to change loss on IP Softphone calls including circuit-switched endpoints. Conference calls of three parties or more are subject to the administrable loss plan, whether those calls involve IP endpoints or not.

Hairpinned audio connections

Hairpinning means rerouting the voice channel connecting two IP endpoints so that the voice channel goes through the TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit packs in IP format instead of through the TDM bus. Communication Manager provides only shallow hairpinning, meaning that only the IP and Real Time Protocol (RTP) packet headers are changed as the voice packets go through the TN2302AP or TN2602AP circuit pack. This requires that both endpoints use the same codec (coder/decoder), a circuit that takes a varying-voltage analog signal through a digital conversion algorithm to its digital equivalent or vice-versa (digital to analog). Throughout this section, when the word hairpin is used, it means shallow hairpinning.

Criteria for hairpinning

Communication Manager uses the following criteria to determine whether to hairpin the connection:

- A point-to-point voice connection exists between two endpoints.
- The endpoints are in the same network region, or in different, interconnected regions.
- A single TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 circuit pack serves both endpoints.
- The endpoints use a single, common codec.

- The endpoints are administered for hairpinning: For shuffled IP calls to use a public IP address (default), set the **Direct IP-IP Audio Connections** field to `y`.
- If the **IP Audio Hairpinning** field is `y` (yes), but during registration the endpoint indicates that it does not hairpinning, then a call cannot be hairpinned. If the **IP Audio Hairpinning** field is `n` (no), but during registration the endpoint indicates that it can support hairpinning, then calls to that endpoint cannot be hairpinned, giving precedence to the endpoint administration.
- Communication Manager uses the criteria to determine whether a shuffled audio connection is possible.
- Both endpoints can connect through the same TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 circuit pack.

Example of a hairpinned call

Hairpinned audio connections:

- Set up within approximately 50 ms
- Preserve the Real-Time Protocol (RTP) header (for example the timestamp and packet sequence number).
- Do not require volume adjustments on Avaya endpoints, however non-Avaya endpoints might require volume adjustment after the hairpinned connection is established.

The *Hairpinned audio connection between two IP endpoints in the same network region* figure is a schematic of a hairpinned audio connection between two IP endpoints in the same network region.

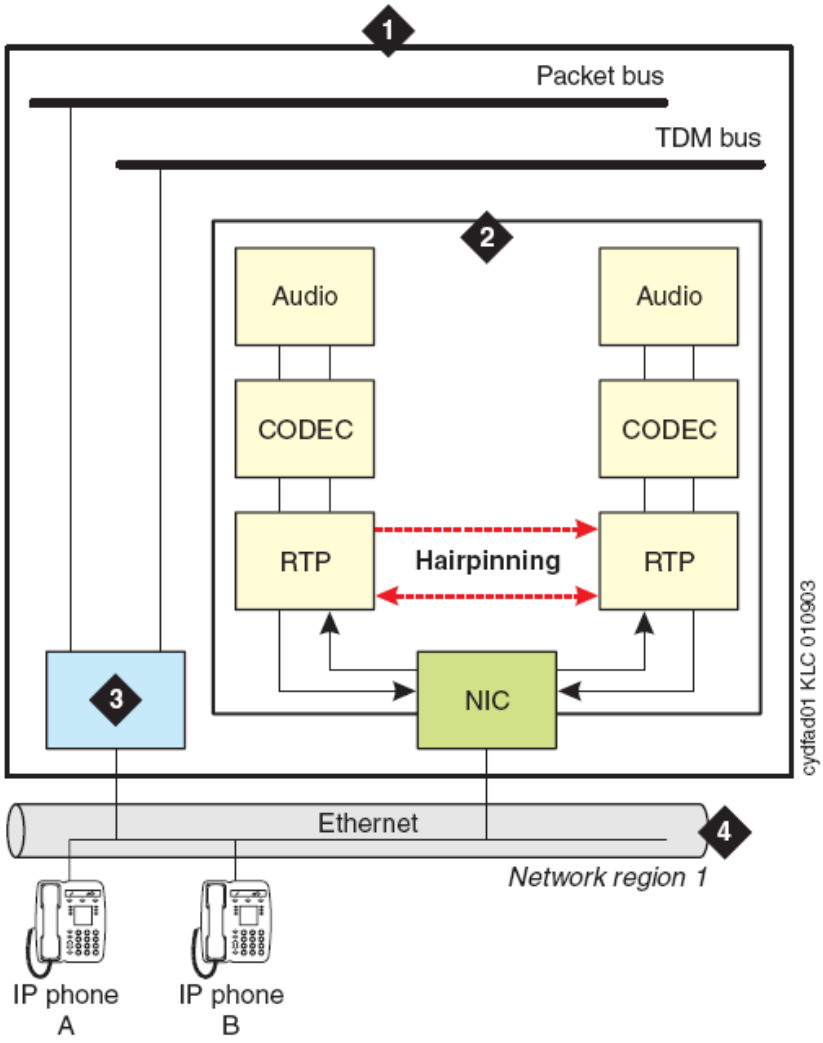


Figure 13: Hairpinned audio connection between two IP endpoints in the same network region

Name	Description
1	Avaya server
2	TN2302AP IP Media Processor and TN2602AP IP Media Resource 320 circuit pack
3	TN799 Control LAN (C-LAN) circuit pack
4	LAN/WAN segment administered in Communication Manager as network region 1

The *Hairpinned audio connection between two IP endpoints in the same network region* figure shows that hairpinned calls bypass the TN2302AP or TN2602AP codec freeing those

resources for other calls. The necessary analog/digital conversions occur in the common codec in each endpoint.

Causes of a hairpinned call to be redirected

Whenever a third party is conferenced into a hairpinned call or a tone or announcement must be inserted into the connection, the hairpinned connection is broken and the call is re-routed over the TDM bus.

Determining which TN2302AP or TN2602AP circuit pack is hairpinning

About this task

Whenever a TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 circuit pack is hairpinning any calls, its yellow LED is on steady. Although there is no simple way to identify all of the extension numbers that are hairpinning through a particular TN2302AP or TN2602AP circuit pack, you can determine which TN2302AP or TN2602AP circuit pack a particular extension is using for hairpinning.

Procedure

1. At the SAT, type **`status station extension`** and press `Enter`to display the Station screen for that extension.
2. Scroll to page 4 of the report.
3. In the **AUDIO CHANNEL** section, check whether there is a value in the **Audio** field under the **Switch Port** column.

   If there is no port listed, then the call is hairpinned.

Hairpinning and shuffling administration interdependencies

The *Hairpinning and shuffling administration* table summarizes the Communication Manager interdependencies that enable hairpinning and shuffling audio connections.

Note:

To use hairpinning or shuffling with either Category A or B features, the **Software Version** field (**`list configuration software-versions`**) must be **R9** or greater.

Important:

Encryption must be disabled for hairpinning to work, because encryption requires the involvement of resources that are not used in the shallow hairpinning connection. This not the case for shuffling, however.

Table 9: Hairpinning and shuffling administration

Administrationscreen	Required customer options [1]	Other interactions
Station	IP StationsRemote Office	Hairpinning is not available if **Service Link Mode** field on ***Station*** screen is **permanent**. Shuffling is available only for the endpoints [2] Avaya IP telephone R2 and Avaya IP Softphone (R2 or newer)
Signaling group	H.323 Trunks	
Inter network region	H.323 TrunksIP Stations Remote Office	User login must have features permissions.
Feature-Related System Parameters	H.323 TrunksIP Stations Remote Office	
1 2		

Direct Media

Communication Manager supports Direct Media for Session Initiation Protocol (SIP) calls. Direct Media signals the direct talk path between SIP endpoints before a call connects.

Direct Media provides the following enhancements to SIP calls:

- Eliminates shuffling of SIP calls after call connects.
- Eliminates clipping on the talk path.
- Reduces the number of signaling messages for each SIP call.

[1] The fields listed in this column must be enabled through the License File. To determine if these customer options are enabled, use the **`display system-parameters customer-options`** command. If any of the fields listed in this column are not enabled, then either the fields for hairpinning and shuffling are not displayed or, in the case of the Inter Network Region Connection Management screen, the second page (the actual region-to-region connection administration) does not display.

[2] Although other vendors' fully H.323v2-compliant products should have shuffling capability, you should test that before administering such endpoints for hairpinning or shuffling. See the section titled Determining whether an endpoint supports shuffling on page 111.

- Reduces Communication Manager processing for each SIP call and increases the capacities of Communication Manager and SIP Busy Hour Call Completions (BHCC).
- Determines the media path early in the call flow and uses fewer media processor resources to configure the system.

Preparing to enable Direct Media

1. Ensure that the call originator is SIP.

   If the call originator is not SIP, Communication Manager does not apply Direct Media to the call.
2. Ensure that you set the following fields in the SIP signalling group screen of the originating SIP User Agent to y:

   - Direct IP-IP Audio Connections

   - Initial IP-IP Direct Media
3. Ensure that the call-originating party does not have a call on hold.

Note:

If you do not meet with the prerequisites for Direct Media, Communication Manager allocates media processors and shuffles the call after the connection is established.

Network Address Translation

Network address translation (NAT) is a function, typically in a router or firewall, by which an internal IP address is translated to an external IP address. The terms intenal and external are generic and ambiguous, and they are more specifically defined by the application. For example, the most common NAT application is to facilitate communication from hosts on private networks to hosts on the public Internet. In such a case, the internal addresses are private addresses, and the external addresses are public addresses.

Note:

This common NAT application does not use a web proxy server, which would be an entirely different scenario.

Another common NAT application is for some VPN clients. The internal address in this case is the physical address, and the external address is the virtual address. This physical address does not necessarily have to be a private address as shown here, as the subscriber could pay for a public address from the broadband service provider. But regardless of the nature of the physical address, the point is that it cannot be used to communicate back to the enterprise through a VPN tunnel. Once the tunnel is established, the enterprise VPN gateway assigns a virtual address to the VPN client application on the enterprise host. This virtual address is part of the enterprise IP address space, and it must be used to communicate back to the enterprise.

The application of the virtual address varies among VPN clients. Some VPN clients integrate with the operating system in such a way that packets from IP applications (for example, FTP

or telnet) on the enterprise host are sourced from the virtual IP address. That is, the IP applications inherently use the virtual IP address. With other VPN clients this does not occur. Instead, the IP applications on the enterprise host inherently use the physical IP address, and the VPN client performs a NAT to the virtual IP address. This NAT is no different than if a router or firewall had done the translation.

Types of Network Address Translation

Static 1-to-1 NAT

Static 1-to-1 NAT is what has already been covered up to this point. In static 1-to-1 NAT, for every internal address there is an external address, with a static 1-to-1 mapping between internal and external addresses. It is the simplest yet least efficient type of NAT, in terms of address preservation, because every internal host requires an external IP address. This limitation is often impractical when the external addresses are public IP addresses. Sometimes the primary reason for using NAT is to preserve public IP addresses, and for this case there are two other types of NAT: many-to-1 and many-to-a-pool.

Dynamic Many-to-1 NAT

Dynamic many-to-1 NAT is as the name implies. Many internal addresses are dynamically translated to a single external address. Multiple internal addresses can be translated to the same external address, when the TCP/UDP ports are translated in addition to the IP addresses. This is known as network address port translation (NAPT) or simply port address translation (PAT). The external server recieves multiple requests coming from a single IP address, but from different TCP/UDP ports. The NAT device remembers which internal source ports were translated to which external source ports.

In the simplest form of many-to-1 NAT, the internal host must initiate the communication to the external host, which then generates a port mapping within the NAT device. The external host can the reply back to the internal host. It is a paradox with this type of NAT (in its simplest form) that the external host cannot generate a port mapping to initiate the communication with the internal host, and without initiating the communication, there is no way to generate the port mapping. This condition does not exist with 1-to-1 NAT, as there is no mapping of ports.

Dynamic Many-to-a-Pool NAT

Many-to-a-pool NAT combines some of the characteristics of both 1-to-1 and many-to-1 NAT. The general idea behind many-to-a-pool NAT is that there should not be a 1-to-1 mapping, but there are too many internal hosts to use a single external address. Therefore, a pool of multiple external addresses is used for NAT. There are enough external addresses in the pool to support all the internal hosts, but not nearly as many pool addresses as there are internal hosts.

Issues between NAT and H.323

Some of the hurdles that NAT presents to H.323 include:

- H.323 messages, which are part of the IP payload, have embedded IP addresses in them.

NAT translates the IP address in the IP header, but not the embedded addresses in the H.323 messages. This is a problem that can be and has been addressed with H.323-aware NAT devices. It has also been addressed with Communication Manager 1.3 and later versions of the NAT feature.

- When an endpoint (IP telephone) registers with the gatekeeper (call server), that endpoint's IP address must stay the same for the duration of the registration.

  This rules out almost all current implementations of many-to-a-pool NAT.

- TCP/UDP ports are involved in all aspects of IP telephony — endpoint registration, call signaling, and RTP audio transmission.

  These ports must remain unchanged for the duration of an event, duration of the registration, or duration of a call. Also, the gatekeeper must know ahead of time which ports will be used by the endpoints for audio transmission, and these ports can vary on a per call basis. These requirements make it very difficult for H.323 to work with port address translation (PAT), which rules out almost all current implementations of many-to-1 and many-to-a-pool NAT.

Communication Manager NAT Shuffling feature

The Communication Manager NAT Shuffling feature permits IP telephones and IP Softphones to work behind a NAT device. This feature was available prior to release 1.3, but it did not work with shuffled calls (**Direct IP-IP Audio** enabled). The NAT feature now works with shuffled calls.

Terms:

The following terms are used to describe the NAT Shuffling feature:

- Native Address — The original IP address configured on the device itself (internal address)
- Translated Address — The IP address after it has gone through NAT, as seen by devices on the other side of the translation (external address)
- Gatekeeper — The Avaya device that is handling call signaling.

  It could be a portal to the gatekeeper, such as a C-LAN, or the gatekeeper itself, such as an S8300D Server.

- Gateway — The Avaya device that is handling media conversion between TDM and IP, such as a MedPro board, G700 VoIP Media Module, or any of the following Branch Gateways:
  - G450
  - G430
  - G350
  - G250

The essence of this feature is that Communication Manager keeps track of the native and translated IP addresses for every IP station (IP telephone or IP Softphone). If an IP station

registration displays with different addresses in the IP header and the RAS message, the call server stores the two addresses and alerts the station that NAT has taken place.

This feature works with static 1-to-1 NAT. It does not work with NAPT, so the TCP/UDP ports sourced by the IP stations must not be changed. Consequently, this feature does not work with many-to-1 NAT. This feature work with many-to-a-pool NAT, if a station's translated address remains constant for as long as the station is registered, and there is no port translation.

The NAT device must perform plain NAT – not H.323-aware NAT. Any H.323-aware feature in the NAT device must be disabled, so that there are not two independent devices trying to compensate for H.323 at the same time.

Rules:

The following rules govern the NAT Shuffling feature. The **Direct IP-IP Audio** parameters are configured on the SAT ip-network-region screen.

- When **Direct IP-IP Audio** is enabled (default) and a station with NAT and a station without NAT talk to one another, the translated address is always used.
- When two stations with NAT talk to one another, the native addresses are used (default) when `Yes` or `Native (NAT)` is specified for **Direct IP-IP Audio**, and the translated addresses are used when Translated (NAT) is specified.
- The Gatekeeper and Gateway must not be enabled for NAT. As long as this is true, they can be assigned to any network region.

Hairpinning and shuffling

You can administer shuffled and hairpinned connections:

- Independently for system-wide applicability
- Within a network region
- At the user level

Hairpinning and shuffling administration

Level	Communication Manager screen	Link to procedure
System	Feature-Related System Parameters	Administering hairpinning and shuffling at the system-level on page 121
Network region	Network Region	Inter-network region connection management on page 121
IP Trunks	Signaling Group	Administering H.323 trunks for hairpinning and shuffling on page 124

Level	Communication Manager screen	Link to procedure
IP endpoints	Station	Administering IP endpoints for hairpinning and shuffling on page 124

Administering hairpinning and shuffling at the system-level

About this task

You can administer hairpinning or shuffling as a system-wide parameter.

Procedure

1. At the SAT, type **`change system-parameters features`** and press `Enter`.
   The system displays the Feature-Related System Parameters screen:
2. For shuffled IP calls to use a public IP address (default), go to the page with IP PARAMETERS and set the **Direct IP-IP Audio Connections** field to **y**.
   Set this field to **n** if you donot want shuffled IP calls to use a public IP address (default). Be sure that you understand the interactions in Hairpinning and shuffling administration interdependencies on page 115 and the notes below.
3. For hairpinned audio connections, type **y** (yes) in the **IP Audio Hairpinning** field, noting the interactions in Hairpinning and shuffling administration interdependencies on page 115 and the notes below.
4. Save the changes.

Note:

The **Direct IP-IP Audio Connections** and **IP Audio Hairpinning** fields do not display if the **IP Stations** field, the **H.323 Trunks** field, and the **Remote Office** field on the Customer Options screen are set to **n**.

Inter-network region connection management

Shuffling and hairpinning endpoints or media processing resources in any given network region is independently administered per network region, which uses a matrix to define the connections between pairs of regions.

The matrix is used two ways:

- It specifies what regions are valid for resource allocation when resources in the preferred region are unavailable.
- When a call exists between two IP endpoints in different regions, the matrix specifies whether those two regions can be directly connected.

Administering hairpinning and shuffling in network regions

Procedure

1. At the SAT type **`change ip-network-region number`** and press `Enter`.
   The system displays the IP Network Region screen.
2. Administer the **IP-IP Direct Audio** fields:
   - The **Intra-region IP-IP Direct Audio** field permits shuffling if both endpoints are in the same region.
   - The **Inter-region IP-IP Direct Audio** field permits shuffling if the two endpoints are in two different regions.

   The defined values for both fields are:
   - **y** -- permits shuffling the call
   - **n** -- does not permit shuffling the call
   - **native**-- the IP address of a telephone itself, or no translation by a Network Address Translation (NAT) device
   - **translated** -- the translated IP address that a Network Address Translation (NAT) device provides for the native address

   Note:
   If there is no NAT device in use at all, then the native and translated addresses are the same. For more information on NAT, see the *Administering Avaya Aura® Communication Manager,03-300509* and *Avaya Aura® Solution Design Considerations and Guidelines,03-603978*.

   Note:
   The hairpinning and shuffling fields on the IP Network Regions screen do not display unless the **IP Stations**, the **H.323 Trunks**, or the **Remote Office** field is set to **y** (yes) on the **Optional Features** (**`display system-parameter customer-options`**) screen. These features must be enabled in the system's License File.
3. Go to page 3 and administer the common codec sets on the Inter Network Region Connection Management screen.
   For more detailed information about the fields on this screen, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

   Note:
   You cannot connect IP endpoints in different network regions or share TN799 C-LAN or TN2032 IP Media Processor resources between/among network regions

unless you make a codec entry in this matrix specifying the codec set to be used. For more information, see IP CODEC sets on page 153.

Note:

Use the **`list ip-codec-set`** command for a list of codecs.

4. Save the changes.

Codecs to administer and select

When an IP endpoint calls another IP endpoint, Communication Manager asks that the 2nd endpoint choose the same codec that the 1st endpoint offered at call setup. However, if the 2nd endpoint cannot match the 1st's codec, the call is set up with each endpoint's administered (preferred) codec, and the data streams are converted between them, often resulting in degraded audio quality because of the different compressions/decompressions or multiple use of the same codec. For more information, see IP CODEC sets on page 153.

When an endpoint (station or trunk) initially connects to the server, Communication Manager selects the first codec that is common to both the server and the endpoint. The Inter Network Region Connection Management screen specifies codec set(s) to use *within* an individual region (intra-region) and a codec set to use *between/among* (inter-region) network regions. Depending upon the network region of the requesting H.323 endpoint or trunk and the network region of the TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 circuit pack:

- If the endpoint and the TN2302AP or TN2602AP are in same region, the administered intra-region codec set is chosen.
- If the endpoint and the TN2302AP or TN2602AP are in different regions, the administered inter-region codec set is chosen.

For example, a region might have its intra-network codec administered as G.711 as the first choice, followed by the other low bit rate codecs. The Inter Network Region Connection Management screen for the inter-network region might have G.729 (a low-bit codec that preserves bandwidth) as the only choice. Initially, when a call is set up between these two interconnected regions, the TN2302AP IP Media Processor or TN2602AP IP Media Resource 320 provides the audio stream conversion between G.711 and G.729. When the media stream is shuffled away from a TDM-based connection, the two endpoints can use only the G.729 codec.

Note:

If you are administering an H.323 trunk that uses Teletype for the Deaf (TTD), use the G.711 codec as the primary choice for those trunks. This ensures accurate TTD tone transmission through the connection.

Administering H.323 trunks for hairpinning and shuffling

Procedure

1. At the SAT, type **change signaling group number** and press Enter.

   The system displays the Signaling Group screen.

2. For shuffled IP calls to use a public IP address (default), set the **Direct IP-IP Audio Connections** field to y.

   Set this field to n if you do not want shuffled IP calls to use a public IP address. Be sure that you understand the interactions in Hairpinning and shuffling administration interdependencies on page 115 and the notes below.

3. For hairpinned audio connections, type y in the **IP Audio Hairpinning** field, noting the interactions in Hairpinning and shuffling administration interdependencies on page 115 and the notes below.

4. Save the changes.

Note:

The hairpinning and shuffling fields on the Signaling Group screen do not display unless either the H.323 Trunks or **Remote Office** field is set to y (yes) on the Optional Features screen. These features must be enabled in the system's License File.

Note:

If you are administering an H.323 trunk that uses Teletype for the Deaf (TTD), use the G.711 codecs as the primary codec choice for those trunks to ensure accurate TTD tone transmission through the connection.

Administering IP endpoints for hairpinning and shuffling

About this task

Shuffle or hairpin is independently administered per endpoint on the Station screen. The specific station types that you can administer for hairpinning or shuffling are:

- All Avaya IP stations
- Other vendors' H.323-compatible stations

Procedure

1. At the SAT, type **change station extension** and press Enter.

   The system displays the Station screen.

2. For shuffled IP calls to use a public IP address (default), set the **Direct IP-IP Audio Connections** field to **y**.

   Set the field as **n** if you donot want shuffled IP calls to use a public IP address. Be sure that you understand the interactions in Hairpinning and shuffling administration interdependencies on page 115 and the notes below.

3. For hairpinned audio connections, type **y** in the **IP Audio Hairpinning** field, noting the interactions in Hairpinning and shuffling administration interdependencies on page 115 and the notes below.

4. Save the changes.

Note:

The hairpinning and shuffling fields on the Station screen do not display unless either the **IP Stations** or **Remote Office** field is set to **y** (yes) on the **Optional Features** (`display system-parameter customer-options`) screen. These features must be enabled in the system's License File.

Note:

The **Direct IP-IP Audio Connections** field cannot be set to **y** if the **Service Link Mode** field is set to **permanent**.

IP station administration for dual-connect

- If an IP station is administered for dual-connect, and if the two extension numbers for that station have differing values administered in their **Direct IP-IP audio Connections** fields, then the station cannot shuffle calls.
- If an IP station is administered for dual-connect, and if the two extension numbers for that station have differing values administered in their **IP-IP Audio Hairpinning** fields, then the station cannot hairpin calls.

IP stations used for call center service-observing

If a Call Center agent is active on a shuffled call, and a Call Center supervisor wants to service-observe the call, the agent might notice the 200 ms break in the speech while the call is redirected to the TDM bus. To avoid the break in speech while the call is redirected, administer the shuffling and hairpinning fields as **n** (no) for stations that are used for service-observing.

IP endpoint signal loss

The amount of loss applied between any two endpoints on a call is administrable. However, the Telecommunications Industry Association (TIA) has published standards for the levels that

IP endpoints should use. The IP endpoints will always transmit audio at TIA standard levels, and expect to receive audio at TIA standard levels. If an IP audio signal goes to or comes from the TDM bus through a TN2302AP Media Processor or TN2602AP IP Media Resource 320, the circuit pack adjusts the levels to approximately equal the levels of a signal to or from a DCP set. By default, IP endpoints are the same loss group as DCP sets, Group 2.

Loss to USA DCP levels

The switch instructs the TN2302AP or TN2602AP circuit pack to insert loss into the signal coming from the IP telephone, and insert gain in the signal going to the IP telephone, to equal the levels of a signal to or from a DCP set.

Note:

The voice level on a shuffled call is not affected by entries administered in the 2-Party Loss Plan screen.

Note:

The loss that is applied to a hairpinned or shuffled audio connection is constant for all three connection types: station-to-station, station-to-trunk, and trunk-to-trunk

Fax, modem, TTY, and H.323 clear-channel calls over IP trunks

Communication Manager uses the Relay mode or the Pass-through mode to transport fax, modem, and Teletypewriter device (TTY) calls over IP interfaces. Communication Manager supports transport of:

- TTY calls over the corporate intranet and the Internet
- Faxes over a corporate intranet or the Internet

  Note:

  Faxes sent to non-Avaya endpoints cannot be encrypted.
- T.38 fax over the Internet, including endpoints connected to non-Avaya systems
- Modem tones over the Internet, including endpoints connected to non-Avaya systems
- Clear-channel data calls over IP

Avaya devices are categorized as category A and category B:

- Category A: Vintage products that use older chip technologies and have slight operational differences from category B devices. G250, G350, and G700 are not being sold.
- Category B: Products that use newer chip technologies.

Category A	Category B
MM760	TN2602
TN2302	G430
G250	G450
G350	
G700	

Relay

In the Relay mode, the firmware on the device detects fax, modem, or TTY tones. To process the call over the IP network, the firmware uses the appropriate modulation protocol for fax or modem, or Baudot transport representation for TTY. The modulation and demodulation process for fax and modem calls reduces bandwidth use over the IP network as compared to the Pass-through mode. The Relay mode improves the reliability of transmission. The correct tones are regenerated before the calls reach the destination endpoint.

Note:

For category A devices, modulation and demodulation reduces the number of simultaneous calls that a device can handle.

Note:

Do not use Avaya-proprietary fax and modem relay protocols. For modem relay applications, use the V.150.1 modem relay protocol. For fax relay applications, use the T.38 fax protocol.

Pass-through

In the Pass-through mode, the firmware on the device detects the tones of the call for fax, modem, or TTY. The firmware then uses G.711 encoding to carry the call over the IP network. The Pass-through mode provides higher quality transmission when endpoints in the network are all synchronized to the same clock source.

Note:

The Pass-through mode increases the bandwidth use of each channel. However, you can make the same number of simultaneous fax or modem calls on the device as the voice calls. For example, with the Pass-through mode on G700 Branch Gateway, you can make 64

simultaneous fax or modem calls instead of only 16 with Relay. The capability applies to only category A devices.

Note:

For the Pass-through mode on a modem and TTY calls over an IP network, the sending and receiving servers must have a common synchronization source. Using a source on the public network, you can establish sychronized clocks.

T.38

In the T.38 mode, the gateway DSP devices or the G650 VoIP boards convert T.30 signals into T.38 packets and send the converted packets to a peer. If the fax endpoint on the far end supports T.30 signaling, the peer converts the packets back into T.30 signals and passes the packets to the fax endpoint. However, if the fax endpoint supports the T.38 protocol, the peer passes the packets directly to the fax endpoint.

T.38 is the preferred industry standard fax protocol. H.323 and SIP trunks support the T.38 protocol.

Communication Manager uses the T.38 protocol for fax transmission over IP network facilities. Communication Manager supports the transition of an existing SIP audio call to a fax call.

During a SIP audio call, when Communication Manager receives a reINVITE message with the audio and image stream, Communication Manager performs one of the following operations:

- If T.38 is administered, Communication Manager accepts the image stream and rejects the audio stream.
- If T.38 is not administered, Communication Manager accepts the audio stream and rejects the image stream.

For more information about FAX over IP, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

V.150.1 Modem Relay

The V.150.1 protocol is an ITU-T recommendation for the transmission of modem data over IP networks. This protocol is the preferred industry-standard modem relay protocol. SIP trunks support the V.150.1 Modem Relay mode. In V.150.1 Modem Relay mode, modem features are implemented according to ITU-T V-series recommendations for interoperation with the non-Avaya trunk-side and line-side modem equipments, and with native-V.150.1 secure IP endpoints. This mode uses the V.150.1 protocol that defines how to transmit modem traffic between modems and telephone devices over an IP network. This mode also supports Modem-over-IP interoperability with SIP endpoints and third-party SIP gateways. This mode uses the

Simple Packet Relay Transport (SPRT) protocol to transmit data between V.150.1 capable endpoints.

Administering fax, TTY, modem, and clear-channel calls over IP trunks

About this task

Using ISDN-PRI trunks, calls are sent either over the public network or over an H.323 or SIP private network to Communication Manager switches.

The endpoints that send and receive the calls must be connected to a private network that uses H.323, SIP, or LAN connections between gateways or port networks.

Procedure

1. Create one or more IP codec sets that enable the appropriate transmission modes for the endpoints on gateways.

   Note:

   Create the fax, modem, TTY, and clear-channel settings, including redundancy, on the second page of the IP Codec Set screen.

2. Assign each codec set to the appropriate network region.
3. Assign the network region to the appropriate devices:
   - TN2302AP or TN2602AP.
   - Avaya G250, G350, G430, G450, or G700 Branch Gateways
4. If the TN2302AP or TN2602AP resources are shared among administered network regions, you must administer internetwork region connections.

Related topics:

Defining IP interfaces (C-LAN, TN2302AP, or TN2602AP Load Balanced) on page 89
IP CODEC sets on page 153
IP network regions on page 156
Manually interconnecting the network regions on page 168

FAX, TTY, modem, and clear channel transmission modes and speeds

Communication Manager provides the following methods for supporting FAX, TTY, modem, and clear channel transmission over IP.

Note:

FAX Relay, FAX Pass-through, TTY Pass-through, Modem Relay, and Modem Pass-through are proprietary solutions that work only between two Avaya supported endpoints, such as media gateways and Communication Manager port networks.

Table 10: FAX, TTY, modem, and clear channel transmission modes and speeds

Mode	Maximum rate	Comments
T.38 FAX Standard (relay only)	9600 bps	This capability is standards-based and uses IP trunks, H.323 or SIP for communicating with non-Avaya systems. Additionally, the T.38 FAX capability uses the User Datagram Protocol (UDP). **Note:** FAX endpoints served by two different Avaya servers can also send T.38 faxes to each other if both systems are enabled for T.38 FAX. In this case, the servers also use IP trunks. A mix of H.323 and SIP call transport segments may be deployed for a single call path. Each time the call traverses from one technology to the other, there is a pair of transcodings. The mix of H.323 and SIP in a fax call path works if one of the end devices is a fax server that integrates using IP. It is important to keep the number of transcoding nodes to three or lessto keep the delay to an acceptable level. If the T.38 FAX sending and receiving endpoints are on port networks or gateways that are registered to the same server, the gateways or port networks revert to Avaya FAX relay mode. The sending and receiving systems must announce the support of T.38 FAX data applications during the H.245 capabilities exchange for H.323 trunks or the SDP media description for SIP trunks. Avaya systems announce support of T.38 FAX if the capability is administered on the Codec Set screen for the region and a T.38-capable media processor was chosen for the voice channel. In addition, for a successful FAX transmission, both systems should support the H.245 null capability exchange (shuffling) to avoid multiple IP hops in the connection. **Note:** To use the T.38 FAX capability, disable modem Relay and modem Pass-through. However, the modem Pass-through mode can use the T.38 FAX capability even if the mode is not diabled. Additionally, the T.38 FAX capability does not support TCP.

Mode	Maximum rate	Comments
		If you experience a packet network loss, assign packet redundancy to T.38 standard faxes to improve packet delivery and robustness of FAX transport over the network. T.38 FAX Standard supports Error Correction Mode (ECM). With ECM, a FAX page is transmitted in a series of blocks that contain frames with packets of data. After receiving the data for a complete page, a receiving fax machine notifies the transmitting fax machine of any frames with errors. The transmitting fax machine then retransmits the specified frames. This process is repeated until all frames are received without errors. If the receiving fax machine is unable to receive an error-free page, the fax transmission can fail and one of the fax machines can disconnect.
FAX Relay	9600 bps	Because the data packets for faxes in relay mode are sent almost exclusively in one direction, from the sending endpoint to the receiving endpoint, bandwidth use is reduced. **Note:** Do not use this proprietary relay protocol. Instead, use T.38 FAX standard or T.38 with fallback to G.711 Pass-through.
FAX Pass-through	V.34 (33.6 kbps)	The transport speed is up to the equivalent of circuit-switched calls and supports G3 and Super G3 FAX rates. **Note:** You can achieve the V.34 speed of 33.6Kbps if the IP transport network has minimum delay and only a few hops. If you are using Super G3 FAX machines as well as modems, do not assign these FAX machines to a network region with an IP Codec set that is modem-enabled as well as FAX-enabled. If its Codec set is enabled for both modem and FAX signaling, a Super G3 FAX machine incorrectly tries to use the modem transmission instead of the FAX transmission. Therefore, assign modem endpoints to a network region that uses a modem-enabled IP Codec set, and assign the Super G3 FAX machines to a network region that uses a FAX-enabled IP Codec set. You can assign packet redundancy in both Pass-through and Relay mode, which means the gateways use packet redundancy to improve packet delivery and robustness of FAX transport over the network.

Mode	Maximum rate	Comments
		The Pass-through mode uses more network bandwidth than the Relay mode. Redundancy increases bandwidth usage even more.
T.38 with fallback to G.711 Pass-through	9600 bps	Communication Manager uses the T.38 protocol for fax transmission only if the protocol can be successfully negotiated with the peer SIP entity. Otherwise, Communication Manager falls back to G.711 for fax transmission. This mode requires a G.711 codec to be administered on the ip-codec-set screen. **Note:** The T.38 with fallback to G.711 Pass-through feature only works over SIP trunks.
TTY Relay	16 kbps	This transport of TTY supports US English TTY (Baudot 45.45) and UK English TTY (Baudot 50). TTY uses RFC 2833 or RFC 2198 style packets to transport TTY characters. Depending on the presence of TTY characters on a call, the transmission toggles between voice mode and TTY mode. The system uses up to 16 kbps of bandwidth, including packet redundancy, when sending TTY characters and normal bandwidth of the audio codec for voice mode.
TTY Pass-through	87-110 kbps	In the Pass-through mode, you can also assign packet redundancy, which means the gateways send duplicated TTY packets to ensure and improve quality over the network. pass-through mode uses more network bandwidth than relay mode. pass-through TTY uses 87-110 kbps, depending on the packet size, whereas TTY relay uses, at most, the bandwidth of the configured audio codec. Redundancy increases bandwidth usage even more.
Modem Relay	V.32 (9600 bps)	The maximum transmission rate can vary with the version of firmware. The packet size for modem relay is determined by the packet size of the codec selected but is always at least 30ms. Also, each level of packet redundancy, if selected, increases the bandwidth usage linearly (that is, the first level of redundancy doubles the bandwidth usage; the second level of redundancy triples the bandwidth usage, and so on). **Note:** Modem over IP in relay mode is currently available only for use by specific secure analog telephones that meet the Future Narrowband Digital Terminal (FNBDT) standard. Do not use this propritary relay

Mode	Maximum rate	Comments
		protocol. Instead, use the V.150.1 standard based relay protocol.
Modem Pass-through	V.34 (33.6 kbps) and V.90/V.92 (43.4 kbps)	Transport speed is dependent on the negotiated rate of the modem endpoints. Though the servers and gateways support modem signaling at v.34 (33.6 bps) or v.90 and v.92 (43.4 kbps), the modem endpoints can automatically reduce transmission speed to ensure maximum quality of signals. V.90 and V.92 are speeds typically supported by modem endpoints only when directly connected to a service provider Internet service. You can also assign packet redundancy in pass-through mode, which means the gateways send duplicated modem packets to improve packet delivery and robustness of FAX transport over the network. pass-through mode uses more network bandwidth than relay mode. Redundancy increases bandwidth usage even more. The maximum packet size for modem pass-through is 20 ms.
Clear-Channel	64 kbps (unrestricted)	The Clear-Channel mode supports only clear channel data. It does not support analog data transmission functionality such as FAX, modem, TTY, or DTMF signals. It is purely clear channel data. In addition, no support is available for echo cancellation, silence suppression, or conferencing. H.320 video over IP using clear channel is supported, if the port networks or the gateways have a reliable synchronization source and transport for framing integrity.
V.150.1 Standard Modem Relay	Need information	V.150.1 protocol is standards-based and uses SIP signaling for communication with non-Avaya systems. This protocol uses one RTP port for sending RFC 2833 tone events, a second RTP port for exchanging State Signaling Events (SSE), and a third RTP port for sending the Simple Packet Relay Transport (SPRT) data packets. The sending and receiving systems negotiate for the support of V.150.1 in the SDP message set of the SIP protocol. The two principle applications are: • commercial telemetry data transport • secure SIP station set voice transport

Considerations for administering FAX, TTY, modem, and Clear-Channel transmission

There are a number of factors to consider when configuring your system for FAX, TTY, modem, and Clear-Channel calls over an IP network:

- Encryption

  You can encrypt most types of relay and pass-through calls using either the Avaya Encryption Algorithm (AEA) or the Advanced Encryption Standard (AES). See Media encryption for FAX, modem, TTY, and clear channel on page 137.

- Bandwidth usage

  Bandwidth usage of modem relay varies, depending on packet size used and the redundancy level selected. The packet size for modem relay is determined by the packet size of the codec selected. Bandwidth usage of modem pass-through varies depending on the redundancy level and packet size selected. The maximum packet size for modem pass-through is 20 ms.

  Bandwidth usage for other modes also varies, depending on the packet size used, whether redundant packets are sent, and whether the relay or pass-through method is used.

  See the *Bandwidth for FAX, modem, and TTY calls over IP networks* table for the bandwidth usage.

- Calls with non-Avaya systems

  For FAX calls where one of the communicating endpoints is connected to a non-Avaya communications system, the non-Avaya system and the Avaya system should both have T.38 defined for the associated codecs.

  Modem and TTY calls over the IP network cannot be successfully sent to non-Avaya systems. Modem V.150.1 calls are interoperable with other systems that also support the V.150.1 protocol.

- Differing transmission methods at the sending/receiving endpoints

  The transmission method or methods used on both the sending and receiving ends of a FAX/modem/TTY/clear channel call should be the same.

  In some cases, a call succeeds even though the transmission method for the sending and receiving endpoints is different. Generally, however, for a call to succeed, the two endpoints must be administered for the same transmission method.

- H.320 Video over IP using Clear Channel

  H.320 Video over IP using Clear Channel is supported, if the Port Networks or the Gateways involved have reliable individual Synchronization Sources and transport for framing integrity of the channels.

- Hardware requirements

  The relay and pass-through capabilities require the following hardware:

  - For Simplex and Duplex servers, certain minimum hardware vintages and firmware versions are required for the TN2302AP or the TN2602AP circuit pack; see the document titled *Avaya Aura® Communication Manager Minimum Firmware/ Hardware Vintages* at http://support.avaya.com.
  - For the G700 and G350 Branch Gateways, the respective firmware version 22.14.0, and VoIP firmware Vintage 40 or greater to support Communication Manager 2.2 is required. An MM760 Media Module with firmware Vintage 40 or greater can be used for additional VoIP capacity. Check the latest firmware on the http://support.avaya.com website.
  - For the Avaya S8300D Servers, the Avaya G250 Branch Gateway, and the Multi-Tech MultiVoIP Gateway, the firmware should be updated to the latest available on the http://support.avaya.com website.
  - For T.38 FAX capability, endpoints on other non-Avaya T.38 compliant communications systems can send FAX calls to or receive FAX calls from endpoints on Avaya systems.

- Multiple hops and multiple conversions

  If a FAX call undergoes two or more conversion cycle, from TDM protocol to IP protocol and back to TDM protocol, the call can fail due to delays in processing through more than one conversion cycle. A modem or TTY call can undergo no more than one conversion cycle, from TDM protocol to IP protocol and back to TDM protocol, on the communication path. If multiple conversion cycles occur, the call fails. As a result, both endpoint gateways and any intermediate servers in a path containing multiple hops must support shuffling for a modem or TTY call to succeed.

  For example, in the following figure a hop occurs in either direction for calls between port network A and Gateway C because the calls are transcoded between point B and point D. In this case, shuffling is required on devices A, B, C, and D.

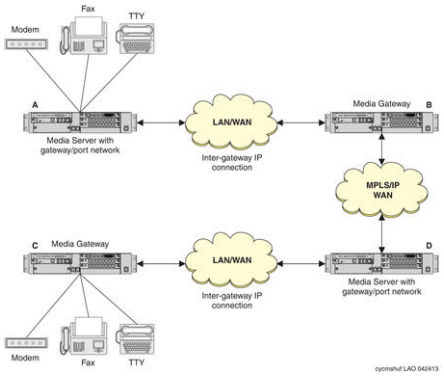


Figure 14: Shuffling for FAX, modem, and TTY calls over IP

Bandwidth for FAX, modem, TTY, and clear channel calls over IP networks

The following table identifies the bandwidth of FAX, modem, TTY, and clear channel calls based on packet sizes used, redundancy used, and whether the relay or pass-through method is used.The values are approximate because bandwidth can vary during each call for multiple reasons.

Table 11: Bandwidth for FAX, modem, and TTY calls over IP networks

Packet Size (in msec)	**Bandwidth (in kbps) (bidirectional)**[3]									
	Redundancy = 0						Redundancy = 1		Red. = 2	Red. = 3
	TTY at G.711	**TTY at G.729**	**TTY at G.723**[4]	**FAX Relay**[5]	**Modem Relay at 9600 Baud**[6]	**Clear Channel FAX/ Modem pass-through**[7] [8]	**FAX Relay**[3] [4]	**Clear Channel FAX/ Modem pass-through**	**FAX Relay**[3] [4]	**FAX Relay**[3] [4]
10	110	54	-	-	-	110	-	221	-	-
20	87	31	-	-	-	87	-	174	-	-
30	79	23	22	25	22.9	-	50	-	75	100
40	76	20	-	-	19.6	-	-	-	-	-
50	73	17	-	-	17.6	-	-	-	-	-
60	72	16	14	-	16.3	-	-	-	-	-
345678										

[3] TTY, Modem Relay, Modem pass-through and FAX pass-through calls are full duplex. Multiply the mode's bandwidth by 2 to get the network bandwidth usage.
[4] TTY at G723 supports packet size 30 and 60 ms.
[5] FAX Relay supports packet size 30ms.
[6] Non-zero redundancy options increase the bandwidth usage by a linear factor of the bandwidth usage when the redundancy is zero.
[7] FAX and Modem pass-through supports packet sizes 10 and 20 ms.
[8] Clear Channel transport supports a packet size of 20 ms.

Media encryption for FAX, modem, TTY, and clear channel

If media encryption is configured, the algorithm used during the audio channel setup of the call will be maintained for most FAX relay and pass-through modes. The exception is the T.38 standard for FAX over IP, for which encryption is not used.

Note:

Encrypted calls reduce Digital Signal Processing (DSP) capacity by 25% compared to non-encrypted calls. DSP capacity reduction does not apply to category B devices. Encryption does not reduce capacity on these platforms.

Encryption is applicable as shown in the following table.

Table 12: Encryption options

Call Type	AEA	AES	SRTP [9]	Transport
Modem Pass-through	Y	Y	Y	RTP (RFC2198)
Modem Relay	Y	N	N	Proprietary
V.150.1 Modem Relay	N	N	N	Simple Packet Relay Transport (SPRT)
FAX Pass-through	Y	Y	Y	RTP (RFC2198)
FAX Relay	Y	(Y) [10]	N	Duplicate Packets
TTY Pass-through	Y	Y	Y	RTP (RFC2198)
TTY Relay	Y	Y	Y	RFC2198
T.38 FAX Standard	(Y) [11]	(Y) [11]	N	T.38 UDPTL Redundancy
Clear Channel	Y	Y	Y	RTP (RFC2198)
91011				

If the audio channel is encrypted, the FAX digital channel is also encrypted except for the limitations described above. AEA-encrypted FAX and modem relay calls that switch back to audio continue to be encrypted using the same key information used at audio call setup.

For the cases of encrypting FAX, modem, and TTY pass-through and TTY relay, the encryption used during audio channel setup is maintained for the call's duration.

The software behaves in the following way for encryption:

[9] See SRTP media encryption on page 138 for a description of the SRTP encryption protocol.

[10] AES encryption in FAX Relay is available only with Avaya equipment (TN2302) with the correct vintages.

[11] The T.38 Fax standard does not support encryption. An enhancement of the T.38 standard enables AES and AEA encryption only with Avaya equipment (TN2302) with the correct vintage.

- For FAX, modem, and TTY pass-through and relay, the VoIP firmware encrypts calls as administered on the CODEC set screen. These calls begin in voice, so voip encrypts the voice channel as administered. If the media stream is converted to FAX, modem, or TTY digital, the VoIP firmware automatically disables encryption as appropriate. When the call switches back to audio, VoIP firmware encrypts the stream again.
- For T.38 FAX, the VoIP firmware encrypts the voice channel as administered on the codec set screen. When the call is converted to FAX, the VoIP firmware automatically turns off encryption. If the call later reverts back to audio, VoIP firmware encrypts the stream again.

SRTP media encryption

Secure Real Time Protocol (SRTP) is a media encryption standard that provides encryption of RTP media streams for SIP and 9600-series IP telephones. SRTP is defined in RFC 3711.

The following SRTP features are supported by Communication Manager, release 4.0 and later:

- Encryption of RTP (optional but recommended)
- Authentication of RTCP streams (mandatory)
- Authentication of RTP streams (optional but recommended)
- Protection against replay

The following SRTP features are currently not supported by Communication Manager:

- Encryption of RTCP streams
- Several automatic rekeying schemes
- Various other options within SRTP which are not expected to be used for VoIP, such as key derivation rates or MKIs

Previous releases of Communication Manager supported AEA and AES media encryption for H.323 calls but no media encryption was available for SIP calls. Starting with release 4.0, SRTP provides encryption and authentication of RTP streams for SIP and provides authentication of RTP and RTCP for SIP and H.323 calls using the 9600-series telephones.

SRTP encryption of FAX and modem relay and T.38 is not supported because they are not transmitted in RTP. For this reason, in the case where an SRTP voice call changes to fax relay, fax will not be encrypted.

SRTP is available only if Media Encryption is enabled in the license file and is activated by IP codec set administration in the same manner as for the other encryption algorithms.

Platforms

The SRTP feature is supported on all Linux-based platforms running Communication Manager and on all versions of SES, regardless of platform, starting with the 4.0 release.

The following gateway platforms also support SRTP:

- TN2602AP Media Resource 320
- MM760
- VoIP Media Modules and on-board VoIP engines (G350 and G250).

Administering SRTP

About this task

Administering SRTP encryption is the same as administering AES and AEA encryption.

Procedure

1. Ensure that media encryption is enabled.

   The Media Encryption? field must be set to ***y*** on the Customer Options form.

2. Administer the Media Encryption type on the ip-codec-set form: **Media Encryption** field.

   This field displayss only if the **Media Encryption over IP** feature is enabled in the license file. Use this field to specify a priority listing of the three possible options for the negotiation of encryption.

3. Administer the ip-network-region form for SIP options:

   Use **Allow SIP URI Conversion?** field to specify whether a SIP Uniform Resource Identifier (URI) is permitted to change. For example, if “sips://” in the URI is changed to sip:// then the call would be less secure but this can be necessary to complete the call. If you enter `n`for no URI conversion, then calls made from SIP endpoints that support SRTP to other SIP endpoints that do not support SRTP will fail. Enter `y`for converting SIP URIs. The default is **y**.

4. You must configure an endpoint (telephone) to use SRTP.

   For an endpoint, set SRTP as media encryption and TLS as transport.

   To enable the SRTP on an endpoint:

   - Use 46xxSettings.txt to set MEDIAENCRYPTION 1,9 (Support 1-srtp-aescm128-hmac80, 9=none as recommended)
   - Use 46xxSettings.txt to set SIPSIGNAL 2 (2 to use Transport protocol as TLS)

Result

For more information about administering SRTP, see Media Encryption on page 177.

Administering SRTP for video signaling

Procedure

1. Type **change system-parameters customer-options**.
   The system displays the Optional Features screen.
2. On page 4 of the Optional Features screen, set the **Media Encryption Over IP** field to `y`.
   This setting is applies both, audio and video SRTP.
3. Type **change system-parameters features**.
   The system displays the Feature-Related System Parameters screen.
4. On page 19 of the Feature-related System Parameters screen, set the **Initial INVITE with SDP for secure calls** field to `y`.
5. Type **change signaling-group n**, where *n* is the signaling group number.
   The system displays the Signaling Group screen.
6. On the Signaling Group screen, set the **Enforce SIPS URI for SRTP** field to `y`.
7. Type **change system-parameters ip-options**.
   The system displays the IP-Options Systems Parameters screen.
8. On page 2 of the IP-Options Systems Parameters screen, set the **Override ip-codec-set for SIP direct-media connections** field to:
   - `n` if you are running Communication Manager 6.3.2 or later.
   - `y` if you are running an earlier release of Communication Manager.
9. Type **change ip-codec-set n**, where *n* is the ip codec set number.
   The system displays the IP Codec Set screen.
10. On the IP Codec Set screen, in the **Media Encryption** section, administer the SRTP options.
    a. In field 1, type `1-srtp-aescm128-hmac80`.
    b. In field 2, type `2-srtp-aescm128-hmac32`.
    c. In field 3, type `none`.

Note:

For the video calls to work on the Best Effort SRTP mode, select **none**.

11. Repeat Step 6 for each ip codec set.

Chapter 6: Voice, Video, and Network quality administration

This chapter provides information about:

- improving voice quality by adjusting the voice packet traffic behavior through an IP network, also known as implementing Quality of Service (QoS).
- Network recovery and survivability

The topics covered are:

Factors causing voice degradation on page 143 introduces the types of voice degradation and their causes.

Quality of Service (QoS) and voice quality administration on page 150 tells you how to administer your Avaya equipment for voice quality and offers suggestions for other network problems.

Media Encryption on page 177 discusses media encryption capabilities, requirements, and administration in Communication Manager.

Network recovery and survivability on page 184 includes information about administering H.248 Link Recovery and the Avaya Policy Manager (APM) and Avaya VoIP Monitoring Manager network monitoring tools.

Note:

Implementing QoS requires administration adjustments to Avaya equipment as well as LAN/WAN equipment (switches, routers, hubs, etc.).

For more information about QoS, see *Avaya Aura® Solution Design Considerations and Guidelines*, 03-603978.

For more information on implementing QoS, see the White Paper, *Avaya IP Voice Quality Network Requirements (LB1500-02)*, at http://www.avaya.com/master-usa/en-us/resource/assets/whitepapers/lb1500-02.pdf.

Factors causing voice degradation

VoIP applications put severe constraints on the amount of end-to-end transfer delay of the voice signal and routing. If these constraints are not met, users complain of garbled or degraded voice quality, gaps, and pops. Due to human voice perception, VoIP applications can afford to randomly lose a few voice packets and the user can still understand the

conversation. However, if voice packets are delayed or systematically lost, the destination experiences a momentary loss of sound, often with some unpleasing artifacts like clicks or pops. Some of the general complaints and their causes are listed in the following table:

Table 13: User complaints and their causes

Complaint	Possible causes and links to information
'Talking over' the far end	• Packet delay and loss on page 145 • Echo on page 145 • Network architecture between endpoint and intermediate node • Switching algorithms
Near-end/ far-end hear(s) echo	• Impedance mismatch • Improper coupling • Codec administration
Voice is too soft or too loud	• PSTN loss • Digital loss • Automatic Gain Control • Conference loss plan
Clicks, pops, or stutters	• Packet loss • Timing drift due to clocks • Jitter • False DTMF detection • Silence supprSurvivable Core serverion algorithms
Voice sounds muffled, distorted, or noisy	• Codec administration • Transducers • Housings • Environment • Analog design

Some of the factors causing voice degradation are:

- Packet delay and loss on page 145
- Echo on page 145
- Transcoding on page 149

Packet delay and loss

The causes of voice degradation include:

- Packet delay (latency)
  - Buffer delays
  - Queuing delays in switches and routers
  - Bandwidth restrictions
- Jitter (statistical average variance in end-to-end packet travel times)
- Packet loss
  - Network overloaded
  - Jitter buffers filled
  - Echo

For a detailed discussion of packet delay and loss, see *Avaya Aura® Solution Design Considerations and Guidelines*, 03-603978.

Tip:

Use a network assessment that measures and solves latency issues before implementing VoIP solutions. For more information, see *Avaya Aura® Solution Design Considerations and Guidelines*, 03-603978.

Echo

When you hear your own voice reflected back with a slight delay, this is echo and it happens for the following reasons:

- Electrical -- from unbalanced impedances or cross-talk
- Acoustical -- introduced by speakerphone or room size

The total round-trip time from when a voice packet enters the network to the time it is returned to the originator is echo path delay. In general, calls over a WAN normally have a longer echo path delay compared to calls over a LAN.

Note:

VoIP itself is not a cause of echo. However, significant amounts of delay and/or jitter associated with VoIP can make echo perceptible that would otherwise not be perceived.

Echo cancellers

Echo cancellers minimize echo by comparing the original voice pattern with the received patterns, and canceling the echo if the patterns match. However echo cancellers are not perfect, especially:

- When the round-trip delay from the echo canceller to the echo reflection point and back is longer than the time that the original (non-echoed) signal is buffered in the echo canceller memory. The larger the echo canceller's memory the longer the signal is held in the buffer, maximizing the number of packets that the canceller can compare in the allotted time.
- During Voice Activity Detection (VAD), which monitors the level of the received signal:
  - An energy drop of at least 3dB weaker than the original signal indicates echo.
  - An energy level 3dB greater indicates far-end speech.

Echo cancellers do not work well over analog trunks and with speakerphones with volume controls that permit strong signals. Although VADs can greatly conserve bandwidth, overly-aggressive VADs can cause voice clipping and reduce voice quality. VAD administration is done on the station screen for the particular IP telephone.

Analog trunks in IP configurations need careful network balance settings to minimize echo. A test tone of known power is sent out and the return signal measured to determine the balance setting, which is critical for reducing echo on IP calls across these trunks.

Echo cancellation plans (TN464HP/TN2464CP circuit packs)

The following summarizes the echo cancellation plans that are available exclusively for the TN464HP/TN2464CP circuit packs. For echo cancellation plans that are available for the TN464GP/TN2464BP circuit packs, see Echo cancellation plans (TN464GP/TN2464BP circuit packs) on page 147.

Echo Cancellation Configuration 1 - TN464HP/TN2464CP

This plan is the recommended choice. It has comfort noise generation and residual echo suppression turned on. During "single talk", background noise and residual echo from the distant station can be suppressed and replaced with comfort noise. The comfort noise substitution reduces the perception of background noise pumping, as observed by the talker. In this plan, the EC direction is chosen to cancel the talker's echo. Since this plan turns on comfort noise and echo suppression, it is similar to EC plans 8 and 9 for the TN464GP/TN2464BP circuit packs.

Echo Cancellation Configuration 2 - TN464HP/TN2464CP

This configuration has comfort noise generation turned off and residual echo suppression turned on. This plan can work well in a quiet background environment. In a noisy background environment, background noise pumping/clipping can be heard by the talker. In this case, EC direction is chosen to cancel the talker's echo. This plan can be a good compromise for a small percent of users, who do not care for the comfort noise and prefer the silence during the

residual echo suppression periods. Since the plan turns off comfort noise and turns on residual suppression, it is similar to EC configurations 1-6 for the TN464GP/TN2464BP circuit packs.

Echo Cancellation Configuration 3 - TN464HP/TN2464CP

This configuration has comfort noise generation and residual echo suppression turned off. This configuration can be a good choice only if EC plans 1 and 2 do not satisfy the user's preferences. Situations that require configuration 3 should be very rare. (For example, the user does not care for the sound of comfort noise nor the pumping/clipping of background noise.) Using this configuration you can hear sound from the earpiece as natural as possible. However, the user can hear residual echo during training periods, or all the time if echo is sufficiently high and residual echo is always present. Convergence can be very slow. Since comfort noise and residual suppression are turned off, this configuration is similar to EC configuration 7 for the TN464GP/TN2464BP circuit packs.

Echo cancellation plans (TN464GP/TN2464BP circuit packs)

Communication Manager supports several echo cancellation (EC) plans for the TN464GP/TN2464BP circuit packs.

Note:

An EC configuration setting can be changed in real time.The change takes effect immediately. That is, it is not necessary to busyout/release the circuit pack – you simply change the setting on the DS1 Circuit Pack screen. This can be done without disruption to existing calls - in fact, you immediately hear the effect of the change.

Important:

When there are TN2302AP or TN2602AP circuit pack(s) and TN464GP/TN2464BP circuit pack(s) being used for a call, the echo canceller on the TN2302AP or TN2602AP is turned off and the echo canceller on the TN464GP/TN2454BP is used instead, because it has the greater echo canceller.

The following summarizes the echo cancellation plans that are available for the TN464GP/TN2464BP circuit packs. For echo cancellation plans that are available exclusively for the TN464HP/TN2464CP circuit packs, see Echo cancellation plans (TN464HP/TN2464CP circuit packs) on page 146.

Echo Cancellation Configuration 1 – Highly Aggressive Echo Control

This configuration can control very strong echo from a distant party. It (as well as Echo Cancellation Configuration 4) provides the most rapid convergence in detecting and correcting echo at the beginning of a call. The initial echo fades faster than the other settings (generally in a small fraction of a second), regardless of the loudness of the talker's voice. EC Configurations 1 and 4 are the same except for loss. EC Configuration 1 has 6dB of loss and EC 4 has 0dB of loss. This makes EC Configuration 1 a good choice for consistently high network signal levels. EC Configuration 1 can cause low-volume complaints and/or complaints of clipped speech utterances, particularly when both parties speak simultaneously (doubletalk). Because EC Configuration 1 relies strongly on echo suppression to help control

echo, pumping of the distant party's background noise can occur and lead to complaints. Prior to Communication Manager Release 2.0, EC Configuration 1 was the default configuration.

The 6dB of loss in EC Configuration 1 is in one direction only and depends on the setting of the **EC Direction** field on the DS1 Board screen. If the direction is set to **inward**, then the 6dB of loss is inserted in the path out from the board towards the T1/E1 circuit. Conversely, if the setting is **outward**, then the 6dB of loss is inserted into the path from the T1/E1 circuit towards the TDM bus.

Echo Cancellation Configuration 2 – Aggressive, Stable Echo Control

This configuration is nearly identical to EC Configuration 1, except that it does not inject an additional 6dB of signal loss, *and* convergence of the echo canceller is slower, but more stable than that provided by EC Configuration 1. If EC Configuration 1 is found to diverge during doubletalk conditions – noticeable by the sudden onset of audible echo, EC Configuration 2 should be used in place of EC Configuration 1. Because the echo canceller converges somewhat slower, some initial echo can be noticeable at the start of a call, while the system is training. EC Configuration 2 can cause complaints of clipped speech utterances, particularly during doubletalk. Because EC Configuration 2 relies strongly on echo suppression to help control echo, pumping of the distant party's background noise can occur and lead to complaints.

Echo Cancellation Configuration 3 – Aggressive, Very Stable Echo Control

This configuration is nearly identical to EC Configuration 2, but is even more stable. Because the echo canceller converges somewhat slower, some initial echo can be noticeable at the start of a call. EC Configuration 3 can cause complaints of clipped speech utterances, particularly during doubletalk. Because EC Configuration 3 relies strongly on echo suppression to help control echo, pumping of the distant party's background noise can occur and lead to complaints.

Echo Cancellation Configuration 4 – Highly Aggressive Echo Control

Echo Cancellation Configuration 4 is identical to EC Configuration 1, but does not provide the 6dB loss option as described for EC Configuration 1. All other comments from EC Configuration 1 apply to EC Configuration 4. EC Configuration 4 can cause complaints of clipped speech utterances, particularly during doubletalk. Because EC Configuration 4 strongly relies on echo suppression to help control echo, pumping of the distant party's background noise can occur, and lead to complaints.

Echo Cancellation Configuration 5 – Very Moderate, Very Stable Echo Control

Echo Cancellation Configuration 5 departs significantly from EC Configurations 1 –4. The echo canceller is slower to converge and is very stable once it converges. Some initial echo can be heard at the beginning of a call. EC Configuration 5 will not, in general, lead to complaints of clipped speech or pumping of the distant party's background noise.

Echo Cancellation Configuration 6 – Highly Aggressive Echo Control

Echo Cancellation Configuration 6 is identical to EC Configuration 4, but reliance on the echo suppressor to control echo is about one-half that of EC Configuration 4. As a result, EC Configuration 6 will not clip speech as much as EC Configuration 4, but can cause somewhat more audible echo, particularly at the start of a call. Some pumping of the distant party's background noise can be perceptible.

Echo Cancellation Configuration 7 – Extremely Moderate & Stable Echo Control

Echo Cancellation Configuration 7 provides very stable and transparent control of weak to low-level echoes. For connections having audible echo at the start of a call, the residual echo can linger for several seconds as the echo canceller converges.

Echo Cancellation Configuration 8 –Aggressive, Very Transparent Echo Control 1

Echo Cancellation Configuration 8 provides aggressive control of echo at the start of a call and more moderate control during the call. Unlike all prior settings, EC Configuration 8 uses comfort noise injection to match the actual noise level of the distant party's speech signal. The effect is one of echo canceller transparency, in which complaints of clipped speech or noise pumping should be few to none. To many people, EC Configuration 8 and EC Configuration 9 will be indistinguishable.

Echo Cancellation Configuration 9 – Aggressive, Transparent Echo Control 2

Echo Cancellation Configuration 9 is nearly identical to EC Configuration 8, but provides somewhat more residual echo control at a slight expense of transparency. To many people, EC Configuration 8 and EC Configuration 9 will be indistinguishable.

Transcoding

When IP endpoints are connected through more than one network region, it is important that each region use the same CODEC, the circuitry that converts an audio signal into its digital equivalent and assigns its companding properties. Packet delays occur when different CODECs are used within the same network region. In this case the IP Media Processor acts as a gateway translating the different CODECs, and an IP-direct (shuffled) connection is not possible.

Bandwidth

In converged networks that contain coexistent voice and data traffic, the volume of either type of traffic is unpredictable. For example, transferring a file using the File Transfer Protocol (FTP) can cause a sharp burst in the network traffic. At other times there can be no data in the network.

While most data applications are insensitive to small delays, the recovery of lost and corrupted voice packets poses a significant problem. For example, users are not concerned if the reception of email or files from file transfer applications is delayed by a few seconds. In a voice call, the most important expectation is the real-time exchange of speech. To achieve this the network resources are required for the complete duration of the call. If in any instance, there are no resources or the network too busy to carry the voice packets, then the destination experiences clicks, pops and stutters. Therefore, there is a continuous need for a fixed amount of bandwidth during the call to keep it real-time and clear.

Quality of Service (QoS) and voice quality administration

Of the VoIP network issues described in the Factors causing voice degradation on page 143 section, delay is the most crucial. And because many of the other causes are highly interdependent with delay, the primary goal is to reduce delay by improving the routing in the network, or by reducing the processing time within the end points and the intermediate nodes.

For example, when delay is minimized:

- Jitter and electrically-induced echo abate.
- Intermediate node and jitter buffer resources are released making packet loss insignificant.

  As packets move faster in the network, the resources at each node are available for the next packet that arrives, and packets will not be dropped because of lack of resources.

Delay cannot be eliminated completely from VoIP applications, because delay includes the inevitable processing time at the endpoints plus the transmission time. However, the delay that is caused due to network congestion or queuing can be minimized by adjusting these Quality of Service (QoS) parameters:

- Layer 3 QoS on page 150
  - DiffServ on page 150
  - RSVP on page 151
- Layer 2 QoS: 802.1p/Q on page 151

These parameters are administered on the IP Network Region screen (see IP network regions on page 156).

Layer 3 QoS

DiffServ

The Differentiated Services Code Point (DSCP) or DiffServ is a packet prioritization scheme that uses the Type of Service (ToS) byte in the packet header to indicate the packet's forwarding class and Per Hop Behaviors (PHBs). After the packets are marked with their forwarding class, the interior routers and gateways use this ToS byte to differentiate the treatment of packets.

A DiffServ policy must be established across the entire IP network, and the DiffServ values used by Communication Manager and by the IP network infrastructure must be the same.

If you have a Service Level Agreement (SLA) with a service provider, the amount of traffic of each class that you can inject into the network is limited by the SLA. The forwarding class is directly encoded as bits in the packet header. After the packets are marked with their forwarding class, the interior nodes (routers & gateways) can use this information to differentiate the treatment of packets.

RSVP

Resources ReSerVation Protocol (RSVP) can be used to lower DiffServ priorities of calls when bandwidth is scarce. The RSVP signaling protocol transmits requests for resource reservations to routers on the path between the sender and the receiver for the voice bearer packets only, not the call setup or call signaling packets.

Layer 2 QoS: 802.1p/Q

802.1p is an Ethernet tagging mechanism that can instruct Ethernet switches to give priority to voice packets.

Caution:

If you change 802.1p/Q on the IP Network Region screen, it changes the format of the Ethernet frames. 802.1p/Q settings in Communication Manager must match similar settings in your network elements.

The 802.1p feature is important to the endpoint side of the network since personal computer -based endpoints must prioritize audio traffic over routine data traffic.

For IEEE standard 802.1Q, you must specify both a virtual LAN (VLAN) and a frame priority at layer 2 for LAN switches or Ethernet switches, for routing based on MAC addresses.

802.1p/Q provides for 8 priority levels and for a large number of Virtual LAN identifiers. Interpretation of the priority is controlled by the Ethernet switch and is usually based on highest priority first. The VLAN identifier permits segregation of traffic within Ethernet switches to reduce traffic on individual links. 802.1p operates on the MAC layer. The switch always sends the QoS parameter values to the IP endpoints. Attempts to change the settings by DHCP or manually are overwritten. The IP endpoints ignore the VLAN on/off options, because turning VLAN on requires that the capabilities be administered on the closet LAN switch nearest the IP endpoint. VLAN tagging can be turned on manually, by DHCP, or by TFTP.

If you have varied 802.1p from LAN segment to LAN segment, then you must administer 802.1p/Q options individually for each network interface. This requires a separate network region for each network interface.

VLANs

Virtual Local Area Networks (VLANs) provide security and create smaller broadcast domains by using software to create virtually-separated subnets. The broadcast traffic from a node that is in a VLAN goes to all the nodes that are members of this VLAN. This reduces CPU utilization and increases security by restricting the traffic to a few nodes rather than every node on the LAN.

Any end-system that performs VLAN functions and protocols is VLAN-aware, although currently very few end-systems are VLAN-aware. VLAN-unaware switches cannot handle VLAN packets (from VLAN-aware switches), and this is why Avaya's gateways have VLAN configuration turned off by default.

Create separate VLANs for VoIP applications. VLAN administration is at two levels:

- Circuit pack-level administration on the IP-Interfaces screen (see Defining IP interfaces (C-LAN, TN2302AP, or TN2602AP Load Balanced) on page 89)
- Endpoint-level administration on the IP Address Mapping screen

Administering endpoints for IP address mapping

Procedure

1. Type **`change ip-network-map`** and press `Enter`.
2. The system displays the IP Address Mapping screen.
3. In the FROM IP Address field, type the starting IP address.
   A 32-bit address (four decimal numbers, each in the range **0-255**).
4. In the TO IP Address field, type the terminating IP address.
   If this field and the **Subnet Mask** field are blank when submitted, the address in the **From IP Address** field is copied into this field. A 32-bit address (four decimal numbers, each in the range **0-255**).
5. In the **or Subnet Mask** field, specify the mask to be used to obtain the subnet work identifier from the IP address.
   If this field is non-blank on submission, then:
   - Mask applied to **From IP Address** field, placing zeros in the non-masked rightmost bits. This becomes the stored "From" address.
   - Mask applied to **To IP Address** field, placing 1's in the non-masked rightmost bits. This becomes the stored "To" address.

     If this field and the **To IP Address** field are blank when submitted, the address in the **From IP Address** field is copied into the **To IP Address** field.

Valid entries: **0-32**, or blank.

6. In the **Region** field, type the network region for the IP address range.
   Valid entries: **1-250** (Enter the network region number for this interface.)
7. In the **VLAN** field, specify the virtual LAN value.
   This field sends the VLAN instructions to IP endpoints such as IP telephones/IP Softphones. This field does not send instructions to the PROCR, C-LAN, or Media Processor boards.
   Valid entries: **0-4095** (specifies the virtual LAN value); **n** (disabled)
8. In the **Emergency Location Extension** field, type a value of 1-7 digits in length for the emergency location extension.
   The default value is blank. (A blank entry typically would be used for an IP softphone dialing in through PPP from somewhere outside your network.)
   If the entry on this screen differs from the value entered in the **Emergency Location Extension** field on the Station screen, then it is the extension entered on this screen that will be sent to the Public Safety Answering Point (PSAP).
9. Save the changes.

IP CODEC sets

In the IP Codec Set screen, specify the type of CODEC used for voice encoding and companding, and compression/decompression. The CODECs on the IP Codec Set screen are listed in the order of preferred use. A call across a trunk between two systems is set up to use the first common CODEC listed.

Note:

The CODEC order must be administered the same for each system of an H.323 trunk connection. The set of CODECs listed does not have to be the same, but the *order* of the listed CODECs must.

In the IP Codec Set screen, define the CODECs and packet sizes used by each IP network region. You can also enable or disable silence suppression for each CODEC in the set. The screen dynamically displays the packet size in milliseconds (ms) for each CODEC in the set, based on the number of 10ms-frames you administer per packet.

Finally, you use this screen to assign the following characteristics to a codec set:

- Whether or not endpoints in the assigned network region can route FAX, modem, TTY, or clear channel calls over IP trunks
- Which mode the system uses to route the FAX, modem, TTY, or clear channel calls
- Whether or not redundant packets will be added to the transmission for higher reliability and quality. Note: For pass-through mode, payload redundancy per RFC2198 is used.

These characteristics must be assigned to the codec set, and the codec set must be assigned to a network region for endpoints in that region to be able to use the capabilities established on this screen.

Caution:

If users are using Super G3 FAX machines as well as modems, do *not* assign these FAX machines to a network region with an IP Codec set that is modem-enabled as well as FAX-enabled. If its Codec set is enabled for both modem and FAX signaling, a Super G3 FAX machine incorrectly tries to use the modem transmission instead of the FAX transmission. Therefore, assign modem endpoints to a network region that uses a modem-enabled IP Codec set, and assign the Super G3 FAX machines to a network region that uses a FAX-enabled IP Codec set.

Administering an IP Codec set

Procedure

1. Type **`change ip-codec-set set#`** and press `Enter`.
   The system displays the IP Codec Set screen.
2. In the **Audio Codec** field, specify an audio CODEC.
3. In the **Silence Suppressi on** field, type `n`.
   Type `y` if you require silence suppression on the audio stream. This can affect audio quality.
4. In the **Frames per Pkt** field, specify frames per packet.
   Enter a value between 1-6.
   The system displays the **Packet Size (ms)** field automatically.
5. In the **Media Encryption** field, specify one of three possible options for the negotiation of encryption.
   the system displays this field only if the Media Encryption over IP feature is enabled. It specifies one of three possible options for the negotiation of encryption. The selected option for an IP codec set applies to all codecs defined in that set.
6. Go to the page 2 of the screen.

Note:

Use these approximate bandwidth requirements to decide which CODECs to administer. These numbers change with packet size, and include layer 2 overhead. With 20 ms packets the following bandwidth is required:

- 711 A-law — 85 kbps
- 711 mu-law — 85 kbps (used in U.S. and Japan)
- 729 — 30 kbps
- 729A/B/AB — 30 kbps audio

7. In the **All Direct-IP Multimedia?** field, type `y` for direct multimedia via the following codecs:
   - H.261
   - H.263
   - H.264 (video)
   - H.224

     H.224.1 (data, far-end camera control).
8. In the **Maximum Bandwidth Per Call for Direct-IP Multimedia** field, enter the unit of measure, kbits or mbits, corresponding to the numerical value entered for the bandwidth limitation.

   The system displays this field only when **Allow Direct-IP Multimedia** is `y`.
9. In the **FAX Mode** field, specify the mode for fax calls.
10. In the **Modem Mode** field, specify the mode for modem calls.
11. In the **TDD/TTY Mode** field, specify the mode for TDD/TTY calls.
12. In the **Clear Channel** field, type the valid entry.
    - If the value is `y`, 64 kbps clear channel data calls is possible for this codec set.
    - If the value is `n`, 64 kbps clear channel data calls is not possible for this codec set.
13. In the **Redundancy** field, perform one of the following:
    - For the call types TTY, fax, or modem that do not use pass-through mode, enter the number of duplicated packets, from 0 to 3, that the system sends with each primary packet in the call. 0 means that you do not want to send duplicated packets.
    - For the clear-channel call type and call types for which you selected the pass-through mode, you can enter either 0 (do not use redundant payloads) or 1 (use redundant payloads).

14. Save the changes.
15. Type **list ip-codec-set** and press Enter.
    The system lists all CODEC sets on the CODEC Set screen.
16. Review your CODEC sets.

IP network regions

Network regions enable you to group IP endpoints and/or VoIP and signaling resources that share the same characteristics. Signaling resources include Media Processor and C-LAN circuit packs. In this context, IP endpoint refers to IP stations, IP trunks, and G150, G250, G350, G430, G450, and G700 Branch Gateways. Some of the characteristics that can be defined for these IP endpoints and resources are:

- Audio Parameters
  - Codec Set
  - UDP port Range
  - Enabling Direct IP-IP connections
  - Enabling Hairpinning
- Quality of Service Parameters:
  - Diffserv settings
    - Call Control per-hop behavior (PHB)
    - VoIP Media PHB
  - 802.1p/Q settings
    - Call Control 802.1p priority
    - VoIP Media 802.1p priority
    - VLAN ID
  - than Best Effort (BBE) PHB
  - RTCP settings
  - RSVP settings
  - Location
- WAN bandwidth limitations
  - Call Admission control - Bandwidth Limitation (CAC-BL)
  - Inter-Gateway Alternate Routing (IGAR)

For more information on ip-network-region, see *Administering Avaya Aura® Communication Manager 03-300509*.

The following sections tell you about:

- Defining an IP network region on page 157
- Inter-Gateway Alternate Routing on page 27
- Dial Plan Transparency on page 28
- Network Region Wizard on page 167
- Manually interconnecting the network regions on page 168
- Inter-network region connections on page 169
- Pair-wise administration of IGAR between network regions on page 169
- Reviewing the network region administration on page 173

Note:

For more information on using network regions, with examples, see the application note Network Regions for Avaya MultiVantage™ Solutions - A Tutorial, which is available at: http://www.avaya.com/gcm/master-usa/en-us/resource/assets/applicationnotes/advantages_of_implem.pdf (requires Adobe Reader). For more information on configuring network regions in Communication Manager, see the application note *Avaya Aura® Communication Manager Network Region Configuration Guide*, which is available at: http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/netw-region-tutorial.pdf (requires Adobe Reader).

Defining an IP network region

About this task

Caution:

Never define a network region to span a WAN link.

Accept the default values for the following screen.

Procedure

1. Type **`change ip-network-region`**.

   The system displays the IP Network Region screen.
2. Complete the fields using the information in IP Network Region field descriptions on page 158.
3. Save the changes.

Caution:

If you change 802.1p/Q on the IP Network Region screen, it changes the format of the Ethernet frames. 802.1p/Q settings in Communication Manager must match those in all of the interfacing elements in your data network.

IP Network Region field descriptions

Name	Description
Region	Network Region number, **1–2000**.
Location	Blank or **1–2000**. If you leave the field blank, the system obtains the location from the cabinet containing the C-LAN that the endpoint is registered through, or the gateway containing through which the endpoint is registered. This applies to IP telephones and softphones.
Name	Describes the region. Enter a character string up to 20 characters.
Authoritative Domain	The network domain of the server.
Stub Network Region	Specifies whether the network region is a core network region or a stub network region. For network regions 251 to 2000, this is a read-only field with a default value **n**. If you are creating a stub network region, then on page 4, in the **dst rgn** field, you must enter the number of the destination core network region that directly connects with this stub network region. **Note:** If you are converting a core network region to a stub network region, you must ensure that the core network region is directly connected with only one core network region. A stub network must have only one direct connection with a core network.
MEDIA PARAMETERS	

Name	Description
Codec Set	Specifies the CODEC set assigned to a region. Enter a value between **1-7** (default is **1**). **Note:** CODEC sets are administered on the CODEC Set screen (see IP CODEC sets on page 153).
UDP Port-Min	Specifies the lowest port number to be used for audio packets. Enter a value between **2-65406** (default is **2048**). **Note:** This number must be twice the number of calls that must be supported plus one, must start with an even number, and must be consecutive. Minimum range is 128 ports. **Caution:** Avoid the range of well-known or IETF-assigned ports. Do not use ports below 1024.
UDP Port-Max	Specifies the highest port number to be used for audio packets. Enter a value between **130-65535** (default is **65535**). **Caution:** Avoid the range of well-known or IETF-assigned ports. Do not use ports below 1024.
DIFFSERVE/TOS PARAMETERS	
Call Control PHB Value	The decimal equivalent of the Call Control PHB value. Enter a value between **0-63**. • Use PHB **46** for expedited forwarding of packets. • Use PHB **46** for audio for legacy systems that only support IPv4 Type-of-Service, which correlates to the older ToS critical setting. • Use PHB **46** if you have negotiated a Call Control PHB value in your SLA with your Service Provider.

Name	Description
Audio PHB Value	The decimal equivalent of the VoIP Media PHB value. Enter a value between **0-63**: • Use PHB **46** for expedited forwarding of packets. • Use PHB **46** for audio for legacy systems that only support IPv4 Type-of-Service, which correlates to the older ToS critical setting.
802.1p/Q PARAMETERS	
Call Control 802.1p Priority	Specifies the 802.1p priority value, and displays only if the **802.1p/Q Enabled** field is **y**. The valid range is **0–7**. Avaya recommends **6** (high). See Caution below this table.
Audio 802.1p Priority	Specifies the 802.1p priority value, and displays only if the **802.1p/Q Enabled** field is **y**. The valid range is **0–7**. Avaya recommends **6** (high). See Caution below this table.
Video 802.1p Priority	Specifies the Video 802.1p priority value, and displays only if the **802.1p/Q Enabled** field is **y**. The valid range is **0–7**.
H.323 IP ENDPOINTS	
H.323 Link Bounce Recovery	**y/n** Specifies whether to enable H.323 Link Bounce Recovery feature for this network region.
Idle Traffic Interval (sec)	**5-7200** Enter the maximum traffic idle time in seconds. Default is **20**.
Keep-Alive Interval (sec)	**1-120** Specify the interval between KA retransmissions in seconds. Default is **5**.
Keep-Alive Count	**1-20** Specify the number of retries if no ACK is received. Default is **5**.
Intra-region IP-IP Direct Audio	**y/n** Enter `y`to save on bandwidth resources and improve sound quality of voice over IP transmissions. Enter `native (NAT)` if the IP address from which audio is to be received for direct IP-to-IP connections within the region is that of the IP telephone/IP Softphone itself (without being translated by NAT). IP telephones must be configured behind a NAT device *before* this entry is enabled.

Name	Description
	Enter `translated (NAT)` if the IP address from which audio is to be received for direct IP-to-IP connections within the region is to be the one with which a NAT device replaces the native address. IP telephones must be configured behind a NAT device *before* this entry is enabled.
Inter-region IP-IP Direct Audio	**y/n** Enter `y`to save on bandwidth resources and improve sound quality of voice over IP transmissions. Enter `translated (NAT)` if the IP address from which audio is to be received for direct IP-to-IP connections between regions is to be the one with which a NAT device replaces the native address. IP telephones must be configured behind a NAT device *before* this entry is enabled. Enter `native (NAT)` if the IP address from which audio is to be received for direct IP-to-IP connections between regions is that of the telephone itself (without being translated by NAT). IP telephones must be configured behind a NAT device *before* this entry is enabled.
IP Audio Hairpinning?	**y/n** Enter `y`for IP endpoints to be connected through the server's IP circuit pack in IP format, without first going through the Avaya TDM bus.
AUDIO RESOURCE RESERVATION PARAMETERS	
RSVP Enabled?	**y/n** Specifies whether or not you have to enable RSVP.
RSVP Refresh Rate (sec)	Enter the RSVP refresh rate in seconds (**1-99**). This field only displays if the **RSVP Enabled** field is set to **y**.
Retry upon RSVP Failure Enabled	Specifies whether to enable retries when RSVP fails (**y/n**). This field only displays if the **RSVP Enabled** field is set to **y**.
RSVP Profile	This field only displays if the **RSVP Enabled** field is set to **y**. You set this field to what you have configured on your network • **guaranteed-service** places a limit on the end-to-end queuing delay from the sender

Name	Description
	tot he receiver. This is the most appropriate setting for VoIP applications. • **controlled-load** (a subset of **guaranteed-service**) provides for a traffic specifier but not the end-to-end queuing delay.
RSVP unreserved (BBE) PHB Value	Provides scalable service discrimination in the Internet without per-flow state and signaling at every hop. Enter the decimal equivalent of the DiffServ Audio PHB value, **0-63**. This field only displays if the **RSVP Enabled** field is set to **y**. **Note:** The “per-flow state and signaling” is RSVP, and when RSVP is not successful, the BBE value is used to discriminate between Best Effort and voice traffic that has attempted to get an RSVP reservation, but failed.

Call Admission Control

Call Admission Control (CAC) is a feature to set a limit on the bandwidth consumption or number of calls between network regions.

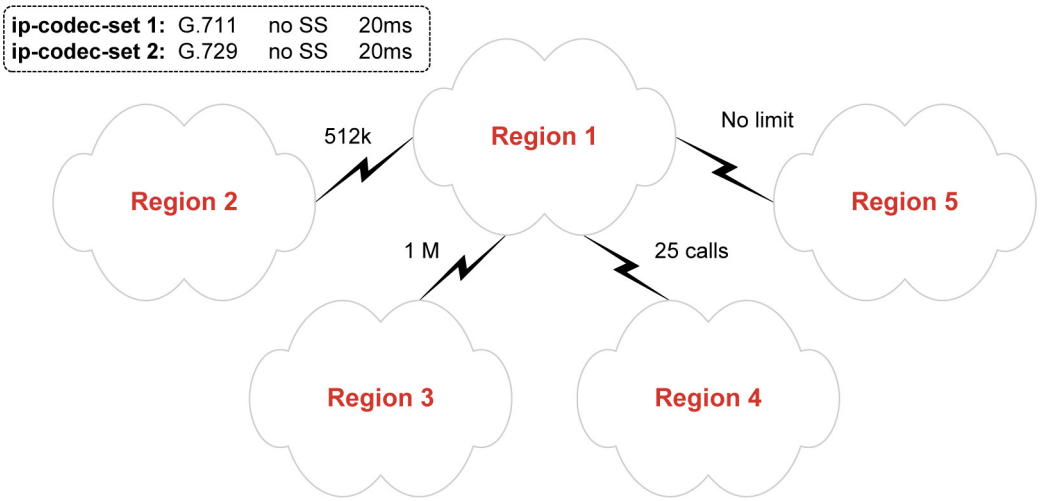
Note:

If SRTP media encryption is used for SIP and H.323 calls, CAC must be adjusted for the additional overhead imposed by the authentication process. SRTP authentication can add 4 (HMAC32) or 10 (HMAC80) bytes to each packet.

The primary use of this feature is to prevent WAN links from being overloaded with too many calls. This is done by setting either a bandwidth limit or a number-of-calls limit between network regions, as follows:

- Bandwidth consumption is calculated using the methodology explained in *Avaya Aura*® *Solution Design Considerations and Guidelines*, 03-603978.
- The L2 overhead is 7 bytes, which is the most common L2 overhead size for WAN protocols.
- The calculated bandwidth consumption is rounded up to the nearest whole number.
- The calculated bandwidth consumption takes into account the actual IP CODEC being used for each individual call. All calls do not use the same CODEC.

- If the administrator chooses not to have the server calculate the bandwidth consumption, the user can enter in a manual limit for the number of calls. However, this manually entered limit is adhered to regardless of the codec being used. Therefore, the administrator must be certain that either all calls use the same CODEC, or that the manual limit takes into account the highest possible bandwidth consumption for the specified inter-region CODEC set.
- If a call between two network regions traverses an intervening network region (for example, a call from 1 to 3 actually goes 1 to 2 to 3), then the call server keeps track of the bandwidth consumed across both inter-region connections, that is, both 1 to 2 and 2 to 3.



The figure above shows a simple hub-spoke network region topology. The WAN link between network regions 1 and 2 has 512kbps reserved for VoIP. The WAN link between network regions 1 and 3 has 1Mbps reserved for VoIP. The link between network regions 1 and 4 is one where the 7-byte L2 overhead assumption would not hold, such as an MPLS or VPN link. In this case, the administration is such that all inter-region calls terminating in region 4 use the G.729 codec (with no SS at 20ms).

Therefore, it is feasible to set a limit on the number of inter-region calls to region 4, knowing exactly how much bandwidth that CODEC consumes (with the MPLS or VPN overhead added). Finally, the link between network regions 1 and 5 requires no limit, either because there are very few endpoints in region 5 or because there is practically unlimited bandwidth to region 5.

The corresponding IP Network Region screens for each network region are shown below.

```
change ip-network-region 1                                    Page   3 of  19

 Source Region: 1     Inter Network Region Connection Management      I        M
                                                                     G  A     e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G     a
 rgn  set   WAN  Units     Total Norm  Prio Shr Regions          CAC  R  L     s
 1    1                                                             all
 2    3     y    Kbits    2000  1000   0   y                       n  ___
 3    1     y    NoLimit                                          n  ___
 4    1     y    NoLimit                                          n  ___
 5    4     y    Kbits    4096  1088   0   y                       n  ___
 6    1     y    NoLimit                                          n  ___
 7    _____                                                         ___
 8    _____                                                         ___
 9    _____                                                         ___
 10   _____                                                         ___
 11   _____                                                         ___
 12   _____                                                         ___
 13   _____                                                         ___
 14   _____                                                         ___
 15   _____                                                         ___
```

```
change ip-network-region 2                                    Page   3 of  19

 Source Region: 2     Inter Network Region Connection Management      I        M
                                                                     G  A     e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G     a
 rgn  set   WAN  Units     Total Norm  Prio Shr Regions          CAC  R  L     s
 1    3     y    Kbits    2000  1000   0   y                       n  ___
 2    1                                                             all
 3    2     y    NoLimit                                          n  ___
 4    _____                                                         ___
 5    _____                                                         ___
 6    _____                                                         ___
 7    _____                                                         ___
 8    _____                                                         ___
 9    _____                                                         ___
 10   _____                                                         ___
 11   _____                                                         ___
 12   _____                                                         ___
 13   _____                                                         ___
 14   _____                                                         ___
 15   _____                                                         ___
```

```
change ip-network-region 3                                    Page   3 of  19

 Source Region: 3     Inter Network Region Connection Management      I       M
                                                                     G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    1___  y    NoLimit                                        n  n ___
 2    2___  y    NoLimit                                        n  ___
 3    1                                                           all
 4    ____                                                        ___
 5    ____                                                        ___
 6    ____                                                        ___
 7    ____                                                        ___
 8    ____                                                        ___
 9    ____                                                        ___
 10   ____                                                        ___
 11   ____                                                        ___
 12   ____                                                        ___
 13   ____                                                        ___
 14   ____                                                        ___
 15   ____                                                        ___
```

```
change ip-network-region 4                                    Page   3 of  19

 Source Region: 4     Inter Network Region Connection Management      I       M
                                                                     G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    1___  y    NoLimit                                        n  ___
 2    ____                                                        ___
 3    ____                                                        ___
 4    1                                                           all
 5    ____                                                        ___
 6    ____                                                        ___
 7    ____                                                        ___
 8    ____                                                        ___
 9    ____                                                        ___
 10   ____                                                        ___
 11   ____                                                        ___
 12   ____                                                        ___
 13   ____                                                        ___
 14   ____                                                        ___
 15   ____                                                        ___
```

```
change ip-network-region 5                                    Page   3 of  19

Source Region: 5     Inter Network Region Connection Management      I       M
                                                                    G  A     e
dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G     a
rgn  set   WAN  Units     Total Norm  Prio Shr Regions          CAC  R  L     s
1    4     y    Kbits    4096  1088    0   y                       n
2
3
4
5    5                                                              all
6
7
8
9
10
11
12
13
14
15
```

Administering DPT

Procedure

1. Enable DPT on the Feature-Related System Parameters screen.
2. Set **Enable Dial Plan Transparency in Survivable Mode** to **y**.
3. Set **COR to Use for DPT** to either **station** or **unrestricted**.

   If set to **station**, the Facility Restriction Level (FRL) of the calling station determines whether that station is permitted to make a trunk call and if so, which trunks it is eligible to access. If set to **unrestricted**, the first available trunk preference pointed to by ARS routing is used.
4. Enable DPT for the appropriate Network Regions.

   On page 2 of the IP Network Region screen, set the **Dial Plan Transparency in Survivable Mode** field to **y**.
5. If not already completed for IGAR, allocate on incoming DID / LDN extension for incoming DPT calls.

   This extension can be shared by IGAR and DPT.
6. As for IGAR, ensure that a sufficient number of trunks are available.

   You do not need to set the maximum number of trunks for DPT.

7. Use existing routing techniques to ensure that an outgoing DPT call from a given Network Region has access to an outgoing trunk.

   The outgoing trunk need not be in the same Network Region as the calling endpoint, as long as the endpoint and trunk Network Regions are interconnected.

Result

For information about DPT, see Dial Plan Transparency on page 28.

Network Region Wizard

The Avaya Network Region Wizard (NRW) is a browser-based wizard. The NWR supports IGAR along with prior support for CAC and codec set selection for inter-connected region pairs. For any system that has several network regions, the use of the wizard can save time for the software specialist or business partner provisioning the system, as well as help to configure the system for optimum IP performance.

The NRW guides you through the steps required to define network regions and set all necessary parameters through a simplified, task-oriented interface. The purpose of the NRW is to simplify and expedite the provisioning of multiple IP network regions, including Call Admission Control via Bandwidth Limits (CAC-BL) for large distributed single-server systems that have several network regions. The NRW is especially valuable for provisioning systems with dozens or hundreds of network regions, for which administration using the System Access Terminal (SAT) scales poorly.

NRW provisioning tasks include:

- Specification and assignment of codec sets to high-bandwidth (intra-region) LANs and lower-bandwidth (inter-region) WANs
- Configuration of IP network regions, including all intra-region settings, as well as inter-region administration of CAC-BL for inter-region links
- Ongoing network region administration by the customer as well as by Avaya technicians and Business Partners to accommodate changes in the customer network following cutover
- Assignment of VoIP resources (C-LANs, TN2302/TN2602 circuit packs, Gateways), and endpoints to IP network regions.

The NRW simplifies and expedites network region provisioning in several ways:

- NRW uses algorithms and heuristics based on graph theory to greatly reduce the repetitive manual entry required by the SAT to configure codecs, and CAC-BL for inter-region links. With the SAT, the number of inter-region links that need to be configured by

the user does not scale well; with the NRW, the number of region pairs that require manual administration will increase *linearly* with the number of regions.
- NRW provides templates of widely applicable default values for codec sets and intra-region parameter settings. Users have the ability to customize these templates with their own default values.
- NRW runs on any Internet browser supported by the Avaya Integrated Management (IM) product line, and takes advantage of browser capabilities to offer user-friendly prompting and context-sensitive online help.

The NRW has its own Job Aid and worksheet (one of Avaya's wizard tools that are available from http://support.avaya.com/avayaiw), and is a standard IM support tool delivered with every Linux-based Communication Manager system.

Manually interconnecting the network regions

Use the **Enable Inter-Gateway Alternate Routing**? field on the Feature-Related System Parameters screen to enable IGAR on a system-wide basis. Using this parameter, IGAR can be quickly disabled without changing/removing other feature administration associated with IGAR. This parameter is included under **System-Wide Parameters** on the Fetaure-Releated System Parameters screen.

If TN799DP (C-LAN) and TN2302AP (IP Media Processor) resources are shared between/among administered network regions, you must define which regions communicate with which other regions and with what CODEC set on the Inter-Network Region Connection Management screen (**`change/display/status ip-network-region`**).

Note:

You cannot connect IP endpoints in different network regions or communicate between/among network regions unless you specify the CODEC set on this screen.

You can also specify for the *Call Admission Control - Bandwidth Limitation* feature:
- Whether regions are directly connected or indirectly connected through intermediate regions.
- Bandwidth limits for IP bearer traffic between two regions using either a maximum bit rate or number of calls.

  When a bandwidth limit is reached, additional IP calls between those regions are diverted to other channels or blocked.

  Typically, the bandwidth limit is specified as the number of calls when the codec set administered across a WAN link contains a single codec. When the codec set administered across a WAN link contains multiple codecs, the bandwidth limit is usually specified as a bit-rate. For regions connected across a LAN, the normal bandwidth limit setting is **nolimit**.

For more information on using network regions, with examples, see the application note *Network Regions for Avaya MultiVantage™ Solutions - A Tutorial*, which is available at: http://

www.avaya.com/gcm/master-usa/en-us/resource/assets/applicationnotes/advantages_of_implem.pdf (requires Adobe Reader). For more information on configuring network regions in Communication Manager, see the application note *Avaya Aura® Communication Manager Network Region Configuration Guide*, which is available at: http://www.avaya.com/master-usa/en-us/resource/assets/applicationnotes/netw-region-tutorial.pdf (requires Adobe Reader). For information on using the Network Region Wizard, see the *Network Region Job Aid*, 14-300283, which is available at http://support.avaya.com.

Inter-network region connections

An **Alternate Routing Extension** field has been added to the second page of the IP Network Region screen. This unassigned extension (up to 7 digits long), together with two other fields are required for each network region to route the bearer portion of the IGAR call. The following must be performed:

- If IGAR is enabled for any row on pages 3 through 19, then the user shall be:
  - Required to enter an IGAR extension before submitting the screen
  - Blocked from blanking out a previously administered IGAR extension
- If IGAR is disabled by the System Parameter, the customer is warned if any of these fields are updated.

Warning:

The IGAR System Parameter is disabled.

Pair-wise administration of IGAR between network regions

An **IGAR** column has been added to the IP Network Region screen for pair-wise configuration of IGAR between network regions. If the field is set to `y` the IGAR capability is enabled between the specific network region pair. If it is set to `n` the IGAR capability is disabled between the network region pair.

The following screen validations must be performed:

- If no IGAR Extension is administered on page 2 of the IP Network Region screen, the user is blocked from submitting the screen, if any network region pair has IGAR enabled.
- If IGAR is disabled using the System Parameter, the customer will be warned, if IGAR is enabled for any network region pair.

  The warning is WARNING: The IGAR System Parameter is disabled.

Normally, the administration between Network Region pairs would have a codec set identified for compressing voice across the IP WAN. Only if bandwidth in the IP WAN is exceeded, and

the **IGAR** field is set to `y`, would the voice bearer be routed across an alternate trunk facility. However, under some conditions you can force all calls to the PSTN.

The forced option can be used during initial installation to verify the alternative PSTN facility selected for a Network Region pair. This option can also be used to move traffic off of the IP WAN temporarily, if an edge router is having problems, or an edge router needs to be replaced between a Network Region pair.

When the codec set type is `pstn` the following fields are defaulted:

- **IGAR** field defaults to `y`. Options: f(orced), n(o), y(es).

  This field must be defaulted to `y` because the Alternate Trunk Facility is the only means of routing the voice bearer portion of the call.

- When the codec set is set to `pstn` the following fields are hidden:

  - Direct-WAN
  - WAN-BW Limits, and
  - Intervening Regions

When the codec set is not `pstn` and not blank, the `IGAR` field is defaulted to `n`.

A `f(orced)` option is supported in the **IGAR** column in addition to the options `n(o)` and `y(es)`.

```
change ip-network-region 3                                    Page 4 of 20

                    Inter Network Region Connection Management          I          M
                                                                       G    A     t
dst   codec direct   WAN-BW-limits   Video       Intervening    Dyn    A    G     c
rgn    set   WAN  Units     Total Norm  Prio Shr Regions        CAC    R    L     e
 1      1     y    256:Kbits                     ___ ___ ___ ___    f
 2      1     n                                 1__ ___ ___ ___    y
 3      1     _                                 ___ ___ ___ ___    n
 4      1     n                                 1__ ___ ___ ___    n
 5      1     n                                 6__ ___ ___ ___    y
 6      1     _     :NoLimit                    ___ ___ ___ ___    y
 7      1     y     10:Calls                    ___ ___ ___ ___    n
 8     pstn   _                                 ___ ___ ___ ___    y
 9     pstn   _                                 ___ ___ ___ ___    y
 10
 11
```

Figure 15: Inter network region connection management

Specify CODEC sets for your shared network regions by placing a CODEC set number in the **codec-set** column. Specify the type of inter-region connections and bandwidth limits in the remaining columns.

In the above example figure, network region 3 is directly connected to regions 6, and 7, and is indirectly connected to regions 2 and 4 (through region 1) and 5 (through region 6).

Port network to network region mapping for circuit packs other than IP circuit packs

Existing IP Media Processor or Resource Modules, for example, the MedPro, C-LAN, and VAL, have assigned IP network regions. The new mapping from cabinet to IP Network Region does not override this administration.

The critical non-IP boards of interest are the trunk circuit packs over which IGAR calls are routed. When an IP connection between two port network/ gateways (PN/MGs) cannot be established, the system tries to establish an IGAR trunk connection between the two PN/MGs. The system tries to use trunks in the specific PN/MG requested. However, because Communication Manager does not require every PN/MG to have PSTN trunks, it be necessary to obtain trunks from another PN/MG. The system can only obtain trunks from a PN/MG in the same Network Region as the one in which the original request was made. This means Communication Manager must let customers associate a port network with a Network Region. This can already be done with Gateways.

Note:

Cabinets connected through a center stage switch (CSS) are required to be in network region 1.

```
display cabinet 1                                                SPE B

                                  CABINET
 CABINET DESCRIPTION
                   Cabinet: 1
             Cabinet Layout: five-carrier
               Cabinet Type: processor
    Number of Portnetworks: 1
     Survivable Remote EPN? n
                  Location: 1               IP Network Region: 1
          Cabinet Holdover: A-carrier-only
                      Room: 1K26_____   Floor: _______  Building: 22_____

CARRIER DESCRIPTION
  Carrier       Carrier Type         Number      Duplicate

      C        port_____________     PN   01
      B        processor________     PN   01
      A        processor________     PN   01
      X        fan______________
      D        dup-sw-node______     SN   01        01E
      E        switch-node______     SN   01        01D
```

Figure 16: IP network region field on cabinet screen to map PNs to network regions

Status of inter-region usage

You can check the status of bandwidth usage between network regions using:**status ip-network-region n** or **n/m**. Using the **n**, the connection status, bandwidth limits, and bandwidth usage is displayed for all regions directly connected to **n**. For regions indirectly connected to **n**, just the connection status is displayed. If regions **n** and **m** are indirectly connected, using **n/m** in the command displays the connection status, bandwidth limits, and bandwidth usage, for each intermediate connection.

The IGAR Now/Today column on the Inter Network Region Bandwidth Status screen displays the number of times IGAR has been invoked for a network region pair, as shown in the *IP network region status screen* figure. Type **status ip-network-regionn**, and press Enterto display the Inter Network Region Bandwidth Status screen.

```
status ip-network-region 2
                  Inter Network Region Bandwidth Status
                                                 Number of   # Times
Src Dst Conn     Conn  BW-Limit  BW-Used(Kbits) Connections  BW-Limit  IGAR
Rgn Rgn Type     Stat              Tx    Rx     Tx    Rx    Hit Today Now/Today
2   1   direct   pass  128 Kbits     xxx   xxx   xxx   xxx     xxx     xxx/ xxx
              Video:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
          Priority:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
2   3   indirect pass  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
              Video:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
          Priority:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
2   4   indirect pass  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
              Video:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
          Priority:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
2   11  indirect pass  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
              Video:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
          Priority:  NoLimit       xxx   xxx   xxx   xxx     xxx     xxx/ xxx
```

Figure 17: IP network region status screen

The numbers in the column titled IGAR Now/Today have the following meanings:

- The first number (up to 3 digits or 999) displays the number of active IGAR connections for the pair of network regions at the time the command was invoked.
- The second number (up to 3 digits or 999) displays the number of times IGAR has been invoked for the pair of network regions since the previous midnight.

Administering the network region on the Signaling Group screen

About this task

Note:

The S8300D Server in Survivable Remote server mode does not support signaling groups.

Procedure

1. Type **change signaling-group group#** and press Enterto display the Signaling Group screen.
2. Type the number of the network region that corresponds to this signaling group in the **Far-end Network Region** field.

   The range of values is: **1-250**.
3. Press Enterto save the changes.

Reviewing the network region administration

Procedure

1. Type **busy signaling-group number** to busy-out the signaling group.
2. Type **change signaling-group number**.

   The sytem displays the Signaling Group screen.
3. In the **Trunk Group for Channel Selection** field, type the trunk group number.

   If there is more than one trunk group assigned to this signaling group, the group entered in this field is the group that accepts incoming calls.
4. Save the changes.
5. Type **release signaling-group number** to release the signaling group.

Setting network performance thresholds

About this task

Note:

The *craft* (or higher) login is required to perform this administration.

Communication Manager gives you control over four IP media packet performance thresholds to help streamline VoIP traffic. You can use the default values for these parameters, or you can change them to fit the needs of your network. These threshold values apply only to IP trunks and do not affect other IP endpoints.

Note:

You cannot administer these parameters unless these conditions are met:

Procedure

1. The **Group Type** field on the Signaling Group screen is **h.323** or **sip**.
2. The **Bypass If IP Threshold Exceeded** field is set to **y** on the Signaling Group screen.

   If bypass is activated for a signaling group, ongoing measurements of network activity collected by the system are compared with the values in the IP-options system-parameters screen. If the values of these parameters are exceeded by the current measurements, the bypass function terminates further use of the network path associated with the signaling group. The following actions are taken when thresholds are exceeded:

   - Existing calls on the IP trunk associated with the signaling group are not maintained.
   - Incoming calls do not arrive at the IP trunks on the bypassed signaling group and are diverted to alternate routes.
   - Outgoing calls are blocked on this signaling group.

     If so administered, blocked calls are diverted to alternate routes (either IP or circuits) as determined by the administered routing patterns.

     Note:

     Use the default values.

Administering network performance parameters

Procedure

1. Type **change system-parameters ip-options**.
   The system displays the IP Options System Parameters screen.
2. Enter values in the following fields suitable for your network needs (defaults shown in the table below):
   - Roundtrip Propagation Delay (ms)

     High: **800** Low: **400**
   - Packet Loss (%)

     High: **40** Low: **15**
   - Ping Test Interval (sec)

     20
   - Number of Pings per Measurement Interval

     10
3. Save the changes.

Enabling or disabling spanning tree

Procedure

1. Open a telnet session on the P330 stack processor, using the serial cable connected to the Console port of the G700.
2. At the **P330-x(super)#** prompt, type **set spantree help** and press Enter.
   The system displays the set spantree commands selection.
   The full set of Spanning Tree commands is displayed in the *Set Spantree commands* figure.

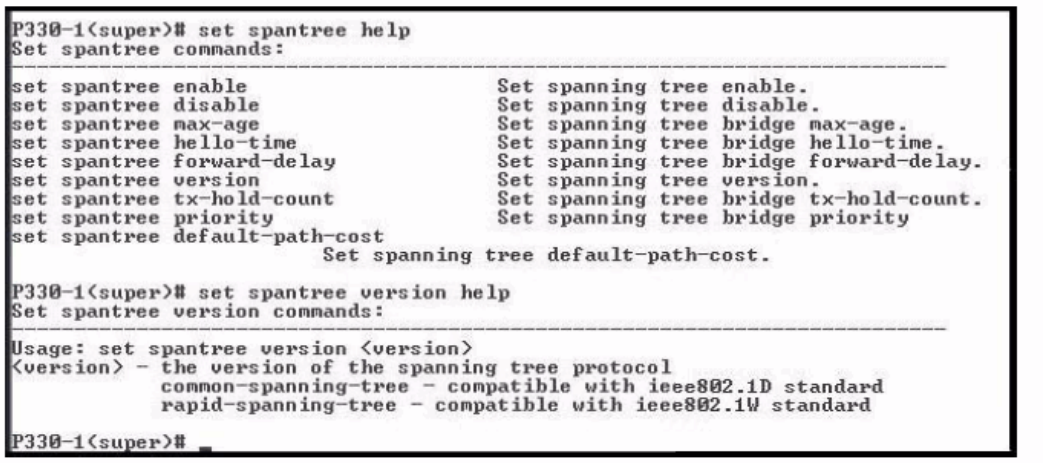


Figure 18: Set Spantree commands

3. To enable Spanning Tree, type **`set spantree enable`** and press `Enter`.
4. To set the version of Spanning Tree, type **`set spantree version help`** and press `Enter`.

   The selection of Spanning Tree protocol commands displays (see the *Set Spantree commands* figure).
5. To set the rapid spanning tree version, type **`set spantree version rapid-spanning-tree`** and press `Enter`.

   The 802.1w standard defines differently the default path cost for a port compared to STP (802.1d). To avoid network topology change when migrating to RSTP, the STP path cost is preserved when changing the spanning tree version to RSTP. You can use the default RSTP port cost by typing the CLI command **`set port spantree cost auto`**.

   Note:

   Avaya P330s now support a “Faststart” or “Portfast” function, because the 802.1w standard defined it. An edge port is a port that goes to a device that cannot form a network loop. To set an **edge-port**, type **`set port edge admin statemodule/port edgeport`**.

Result

For more information on the Spanning Tree CLI commands, see the *Avaya P330 User’s Guide* at http://support.avaya.com.

Jitter buffers

Since network packet delay is usually a factor, jitter buffers should be no more than twice the size of the largest statistical variance between packets. The best solution is to have dynamic

jitter buffers that change size in response to network conditions. Avaya equipment uses dynamic jitter buffers.

- Check for network congestion
- Bandwidth too small
- Route changes (can interact with network congestion or lack of bandwidth)

UDP ports

With Communication Manager you can configure User Datagram Protocol (UDP) port ranges that are used by VoIP packets. Network data equipment uses these port ranges to assign priority throughout the network. Communication Manager can download default values to the endpoint when those values are not provided by the endpoint installer or the user.

Media Encryption

To provide privacy for media streams that are carried over IP networks, Communication Manager supports encryption for IP bearer channel voice data transported in Real Time Protocol (RTP) between any combination of gateways and IP endpoints.

Digitally encrypting the audio (voice) portion of a VoIP call can reduce the risk of electronic eavesdropping. IP packet monitors, sometimes called sniffers, are to VoIP calls what wiretaps are to circuit-switched (TDM) calls, except that an IP packet monitor can watch for and capture unencrypted IP packets and can play back the conversation in real-time or store it for later playback.

With media encryption enabled, Communication Manager encrypts IP packets before they traverse the IP network. An encrypted conversation sounds like white noise or static when played through an IP monitor. End users do not know that a call is encrypted because there are:

- No visual or audible indicators to indicate that the call is encrypted.
- No appreciable voice quality differences between encrypted calls and non-encrypted calls.

Limitations of Media Encryption

Security alert:

Be sure that you understand these important media encryption limitations:

- Any call that involves a circuit-switched (TDM) endpoint such as a DCP or analog telephone is vulnerable to conventional wire-tapping techniques.
- Any call that involves an IP endpoint or gateway that does not support encryption can be a potential target for IP monitoring. Common examples are IP trunks to 3rd-party vendor switches.
- Any party that is not encrypting an IP conference call exposes all parties on the IP call between the unencrypted party and its supporting media processor to monitoring, even though the other IP links are encrypting.

Types of media encryption

Avaya Encryption Algorithm (AEA) and Advanced Encryption Standard (AES) are supported by most Avaya IP endpoints. The Secure Real Time Protocol (SRTP) encryption standard is supported by SIP endpoints and trunks and by the 9600-series telephones.

The *Media encryption support* table lists the telephones and Communication Manager releases that support each type of media encryption.

Table 14: Media encryption support

	Media Encryption Type		
	AEA	**AES**	**SRTP**
Communication Manager release	Avaya Aura® CM 1.3 and later	Avaya Aura® CM 2.0 and later	Avaya Aura® CM 4.0 and later
Avaya IP telephones:			
4601	Y	Y	N
4602	Y	Y	N
4606	Y	N	N
4610SW	Y	Y	N
4612	Y	N	N
4620	Y	Y	N
4620SW / 4621SW / 4622SW / 4625SW / 4630SW	Y	Y	N
4624	Y	N	N
4630	Y	N	N
4690	N	Y	N
1600-series IP telephones	N	Y	N
96xx and 96x1 IP telephones	N	Y	Y

	Media Encryption Type		
	AEA	AES	SRTP
96xx and 96x1 SIP endpoints	N	N	Y
IP Softphone	Y	Y	N
IP Softphone for Windows Mobile	Y	Y	N
IP SoftConsole	Y	N	N
IP Agent	Y	Y	N
TN2302AP IP Media Processor circuit pack	Y	Y	N
TN2602AP IP Media Resource 320 circuit pack	Y	Y	Y
VoIP elements of branch gateways	Y	Y	Y
Avaya one-X® Communicator	N	Y	Y
OSPC	Y	N	N
Avaya 3616 / 3620 / 3626 / 3641 / 3645	N	N	N
Avaya 3631	N	Y	N
Avaya 16CC (Call Center) SIP telephone	N	N	Y

License file

Media Encryption does not work unless the server has a valid license file with Media Encryption enabled. First check the current license file and if Media Encryption is not enabled, then you must install a license file with Media Encryption enabled.

Determining whether Media Encryption is enabled in the current License File

Procedure

1. Type **`display system-parameters customer-options`** and press `Enter`.
   The system displays the Optional Features screen.
2. Scroll to the page with the **Media Encryption Over IP?** field and verify that the value is ***y***.

Note:

Media Encryption is enabled by default in the U. S. and other countries unless prohibited by export regulations.

Administering Media Encryption for IP Codec Sets

About this task

The IP Codec Set screen enables you to administer the type of media encryption, if any, for each codec set.

Note:

IP endpoints do not require any encryption administration, and end users do not have to do anything to use media encryption

Note:

See IP Network Region field descriptions on page 158 for a description of the fields on the IP Codec Set screen.

Procedure

1. At the SAT type **`change ip-codec-set number`** and press `Enter`.

   The system displays the IP Codec Set screen.

2. Enter up to three media encryption types.

   Note:

   The option that you select for the **Media Encryption** field for each codec set applies to all codecs defined in that set.

   Note:

   This field is hidden if the **Media Encryption Over IP?** field on the Customer Options screen is *n*. The **Media Encryption** field displays only if the **Media Encryption over IP** feature is enabled in the license file (and displays as *y* on the Customer Options screen).

   The **Media Encryption** field specifies one, two, or three options for the negotiation of encryption — in this example, one of the modes of **SRTP**, **aes**, and **aea**. You can specify no encryption by entering **none** in the **Media Encryption** field. The order in which the options are listed signifies the preference of use, similar to the list of codecs in a codec set. Two endpoints must support at least one common encryption option for a call to be completed between them.

   The selected options for an IP codec set applies to all codecs defined in that set.

   Note:

   The initial default value for this field is *none* when the **Media Encryption Over IP?** field in the Optional Features screen (on the Customer Options screen) is

enabled (*y*) for the first time. If this field is *n*, the **Media Encryption** field on the IP Codec Set screen is hidden and functions as if *none* was selected.

Media Encryption Field Values (IP Codec Set)

Name	Description
aes	Advanced Encryption Standard (AES), a standard cryptographic algorithm for use by U.S. government organizations to protect sensitive (unclassified) information. AES reduces circuit-switched-to-IP call capacity by 25%.
aea	Avaya Encryption Algorithm. AEA is not as secure an algorithm as AES but call capacity reduction with AEA is negligible. Use this option as an alternative to AES encryption when: • All endpoints within a network region using this codec set must be encrypted. • All endpoints communicating between two network regions and administered to use this codec set must be encrypted.
SRTP — several encryption modes	SRTP provides encryption and authentication of RTP streams for calls between SIP-SIP endpoints, H.323-H.323 endpoints, and SIP-H.323 endpoints. SIP endpoints cannot use AEA or AES encryption.
none	Media stream is unencrypted. This option prevents encryption when using this codec set and is the default setting when Media Encryption is not enabled.

Administering Media Encryption for signaling groups

Procedure

1. Type **`change signaling-group number`**.
   The system displays the Signaling Group screen.

2. To enable Media Encryption on trunk calls using this signaling group, in the **Media Encryption?** field, type `y`.

   Note:

   Leaving this field in the default state (n) overrides the encryption administration on the IP Codec Set screen or any trunk call using this signaling group. That is, if the IP codec set that is used between two networks is administered as aes or aea, then a call between two endpoints over a H.323 trunk using this IP codec set fails because there is no voice path. This system does not display this field if the **Media Encryption Over IP?** field is `n` on the Customer Options screen.

3. Type an 8- to 30-character string in the **Passphrase** field.

   This string:

   - Must contain at least 1 alphabetic and 1 numeric symbol
   - Can include letters, numerals, and!&*?;'^(),.:-
   - Is case-sensitive

   You must administer *the same passphrase* on both signaling group forms at each end of the IP trunk connection. For example, if you have two systems A and B with trunk A-B between them, you must administer both Signaling Group forms with *exactly the same passphrase* for the A-to-B trunk connection.

   If you have previously administered a passphrase, a single asterisk (*) displays in this field. If you have not administered a passphrase, the field is blank.

   The **Passphrase** field does not appear if either the:

   - **Media Encryption Over IP?** field on the Customer Options screen is `n`.

   or

   - **Media Encryption?** field on the Signaling Group screen is `n`.

Viewing encryption status for stations and trunks

About this task

The current status of encryption usage by stations and trunks can be viewed using the **`status station`** and **`status trunk`** commands.

Procedure

1. To check media encryption usage for a station, enter **`status station<extension>`**, and go to the Connected Ports page.

   This screen shows that a port is currently connected and using a G711 codec with SRTP media encryption.

2. To check media encryption usage for a trunk, enter **status trunk<group/member>**.

   A display screen similar to the status station screen shows the trunk information.

Legal wiretapping

If you receive a court order requiring you to provide law enforcement access to certain calls placed to or from an IP endpoint, you can administer Service Observing permissions to a selected target endpoint. Place the observer and the target endpoint in a unique Class of Restriction (COR) with exactly the same properties and calling permissions as the original COR, otherwise the target user might be aware of the change.

For more information about Service Observing, see *Service Observing* in the *Media Encryption interactions* table.

Possible failure conditions

Using Media Encryption in combination with an administered security policy might lead to blocked calls or call reconfigurations because of restricted media capabilities. For example, if the IP codec set that is used between two network regions is administered as **aes** or **aea**, and if a call between two endpoints (one in each region) that do not support at least one common encryption option is set up, then there is no voice path.

Interactions of Media Encryption with other features

Media Encryption does not affect most Communication Manager features or adjuncts, except for those listed in the *Media Encryption interactions* table.

Table 15: Media Encryption interactions

Interaction	Description
Service Observing	You can Service Observe a conversation between encrypted endpoints. The conversation remains encrypted to all outside parties except the communicants and the observer.
Voice Messaging	Any call from an encryption-enabled endpoint is decrypted before it is sent to a voice messaging system. When the TN2302AP IP Media Processor circuit pack receives the encrypted voice stream, it decrypts the packets before sending them to the voice messaging system, which then stores the packets in unencrypted mode.

Interaction	Description
Hairpinning	Hairpinning is not supported when one or both media streams are encrypted, and Communication Manager does not request hairpinning on these encrypted connections.
VPN	Media encryption complements virtual private network (VPN) security mechanisms. Encrypted voice packets can pass through VPN tunnels, essentially double-encrypting the conversation for the VPN “leg” of the call path.
H.323 trunks	Media Encryption behavior on a call varies based on these conditions at call set up: • Whether shuffled audio connections are permitted • Whether the call is an inter-region call • Whether IP trunk calling is encrypted or not • Whether the IP endpoint supports encryption • The media encryption setting for the affected IP codec sets These conditions also affect the codec set that is available for negotiation each time a call is set up. T.38 packets can be carried on an H.323 trunk that is encrypted; however the T.38 packet is sent in the clear.

Network recovery and survivability

This covers the following topics:

- Network management on page 184
- H.248 link loss recovery on page 186
- Administrable IPSI Socket Sanity Timeout on page 195
- Survivable Core Servers on page 196
- QoS policies on page 185
- Monitor network performance on page 185

Network management

Network management is the practice of using specialized software tools to monitor and maintain network components. Proper network management is a key component to the high availability of data networks.

The two basic network management models are:

- Distributed. Specialized, nonintegrated tools to manage discrete components.
- Centralized. Integrated network management tools and organizations for a more coherent management strategy.

Two integrated management tools, Avaya VoIP Monitoring Manager and Avaya Policy Manager are briefly described in this section.

For a detailed discussion of Avaya's network management products, common third-party tools, and the distributed and centralized management models, see *Avaya Aura® Solution Design Considerations and Guidelines*, 03-603978.

Monitor network performance

Using the Avaya VoIP Monitoring Manager, a VoIP Network Quality monitoring tool, you can monitor the following quality-affecting network factors:

- Jitter levels
- Packet loss
- Delay
- CODECs used
- RSVP status

QoS policies

Avaya Policy Manager is a network management tool for controlling Quality of Service (QoS) policies in your IP voice network consistently:

- Avaya Policy Manager helps you implement QoS policies consistently for both the data and the voice networks.
- QoS policies are assigned according to network regions and are distributed through the Enterprise Directory Gateway to your systems and to routers and switching devices.

The following figure illustrates how Avaya Policy Manager works:

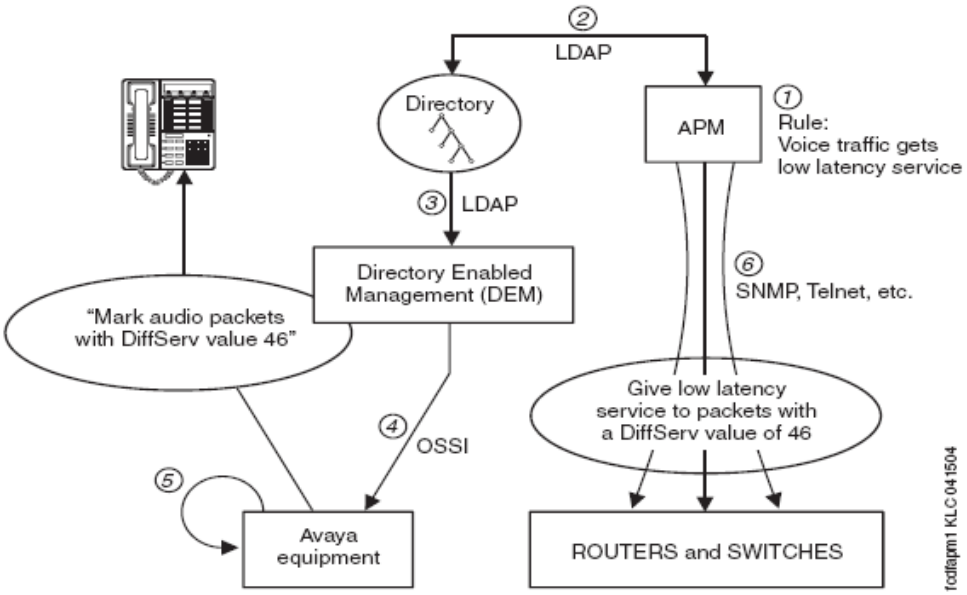


Figure notes:

1. **Business rule established in Avaya Policy Manager**
2. **Avaya Policy Manager uses LDAP to update Communication Manager**
3. **Directory Enabled Management (DEM) identifies the change in the directory.**
4. **EDG updates Communication Manager administration through the Ethernet switch**
5. **Communication Manager tells the Media Processor, C-LAN, and IP Phones to mark audio packets with DSCP=46.**
6. **Avaya Policy Manager distributes policy information to other network devices, including low latency service for DiffServ value of 46.**

Figure 19: Avaya Policy Manager application sequence

For more information about Avaya Policy Manager, go to the Avaya Support website at http://support.avaya.com.

H.248 link loss recovery

H.248 Link Loss Recovery is an automated way in which the gateway reacquires the H.248 link when it is lost from either a primary call controller or an Survivable Remote server. The H.248 link between a server running Communication Manager and a gateway, and the H.323 link between a gateway and an H.323-compliant IP endpoint, provide the signaling protocol for:

- Call setup
- Call control (user actions such as Hold, Conference, or Transfer) while the call is in progress
- Call tear-down

If the link goes down, Link Recovery preserves any existing calls and attempts to re-establish the original link. If the gateway/endpoint cannot reconnect to the original server/gateway, then

Link Recovery automatically attempts to connect with alternate TN799DP (C-LAN) circuit packs within the original server's configuration or to a Survivable Remote server.

Overlap with the Auto Fallback to Primary feature occurs when the Link Loss Recovery starts while the gateway is trying to migrate back to the primary, with its new registration message indicating that service is being obtained from elsewhere.

A rare condition can exist in which there is an outstanding gateway registration to the primary while the link to the Survivable Remote server is lost. The gateway awaits a denial or acceptance from the primary call controller. If it is an acceptance, then the Link Loss Recovery is terminated, and the gateway is serviced by the primary call controller. If it is a denial, then the gateway immediately sends a new registration to the primary call controller indicating no service, and the existing H.248 Link Loss Recovery feature takes over.

These features are similar in that they both attempt to return service to the primary call controller; however, Link Loss Recovery does it based upon a link failure, whereas auto fallback to primary does it based upon a working fragmented network.

Auto fallback to primary controller for branch gateways

The intent of the auto fallback to primary controller feature is to return a fragmented network, in which a number of Branch Gateways are being serviced by one or more Survivable Remote servers, to the primary server in an automatic fashion. This feature is targeted towards all branch gateways. By migrating the gateways back to the primary automatically, the distributed telephony switch network can be made whole sooner without human intervention.

The auto-fallback migration, in combination with the connection preservation feature for H.248 gateways is connection-preserving. Stable connections are preserved; unstable connections (such as ringing calls) are not. There still can be a very short interval without dialtone for new calls.

The gateway presents a new registration parameter that indicates that Service is being obtained from an Survivable Remote server, and indicates the number of active user calls on the gateway platform. The server administers each gateway to have its own set of rules for Time of Day migration, enable/disable, and the setting of call threshold rules for migration.

Using this feature, the administrator can define any of the following rules for migration:

- The gateway should migrate to the primary automatically, or not.
- The gateway should migrate immediately when possible, regardless of active call count.
- The gateway should only migrate if the active call count is 0.
- The gateway should only migrate within a window of opportunity, by providing day of the week and time intervals per day. This option does not take call count into consideration.
- The gateway should be migrated within a window of opportunity by providing day of the week and time of day, or immediately if the call count reaches 0. Both rules are active at the same time.

Internally, the primary call controller gives priority to registration requests from those gateways that are currently not being serviced by an Survivable Remote server. This priority is not administrable.

There are several reasons for denying an auto-fallback, which can result from general system performance requirements, or from administrator-imposed requirements. General system performance requirements can include denial of registration because:

- Too many simultaneous gateway registration requests

Administrator-imposed requirements for denial of a registration can include:

- Registrations restricted to a windowed time of day
- Migration restricted to a condition of 0 active calls, that is, there are no users on calls within the gateway in question.
- The administered minimum time for network stability has not been exceeded.

Other characteristics of this feature include:

- This feature does not preclude an older GW firmware release from working with Communication Manager 6.0 or vice versa. However, the auto-fallback feature would not be available.

  For this feature to work, the call controller is required to have Communication Manager 6.0, while the gateway is required to have the GW firmware available at the time of the Communication Manager 6.0 release.
- Existing branch gateways are the targets.
- Survivable Remote server operation is completely unaffected.

  The Survivable Remote server simply sees that a particular gateway has lost its connection with the Survivable Remote server. The existing H.248 Link Loss Recovery algorithm on the Survivable Remote server cleans up all outstanding call records within the Survivable Remote server after the prescribed time interval.

For each gateway, the following administration must be performed:

- Adding Recovery Rule to Gateway screen on page 191
- System Media Parameters Gateway Automatic Recovery Rule screens on page 192 to schedule the auto-fallback within the system-parameters area.

Basic feature operation

The following illustrate the basic operation of the auto-fallback to primary for branch gateways feature. While not exactly so, the steps are approximately sequential.

- The gateway/server *by default* has this feature disabled.

If the gateway is initially registered with an older server, the version information exchange is sufficient for the gateway to know not to attempt to fallback to the primary automatically.

- By means of administration on the server, this feature can be enabled for any or all gateways controlled by that server.

  The *enable/disable* administration on the server determines whether the server will *accept/deny* registration requests containing the new parameter that service is being obtained from an Survivable Remote server. The gateway continuously attempts to register with the server, however, even if the server has been administered never to accept the registration request (that is, the auto-fallback feature is disabled on the server). In such a case, a manual return of the gateway is required, which generates a different registration message that is accepted by the server.

  Note:

  There is still value in receiving the registration messages when auto-fallback is disabled on the server, and that value is to see the stability of the network over time, since those messages act as “keep-alive” messages.

- The permission-based rules that include time of day and context information are only known to the server.

  There is no need for the Survivable Remote server to have any of these translations.

- When associated with a primary controller running Communication Manager 3.0, the gateway attempts to register with the primary controller whenever it is connected to an Survivable Remote server.

  This registration attempt happens every 30 seconds, once the gateway is able to communicate with the primary controller. The registration message contains an element that indicates:

  - that the gateway is being serviced by an Survivable Remote server, and
  - the number of active user calls on that gateway.

- Upon the initial registration request, the primary controller initializes the encrypted TCP link for H.248 messaging.

  This is performed regardless of whether that initial registration is honored or not, and that encryption is maintained throughout the life of the registration requests. The encryption is also maintained once a registration is accepted by the primary controller. Encryption of the signaling link is performed at the outset during this automatic fallback process to ensure the security of the communication between the primary call controller and the gateway.

- The primary controller, based upon its administered rules, can allow or deny a registration.

If the primary controller gets a registration message without Service State information, for example, an older gateway, or if a new gateway states it does not have service, then the primary honors those registration requests above all others immediately.

- If the registration is denied, the gateway continues to send the registration message every 30 seconds, which acts as a *de facto* '"keep-alive" message.
- The gateway constantly monitors the call count on its platform, and asynchronously sends a registration message whenever 0 context is achieved.
- Once the registration message is accepted by the primary, then the H.248 link to the Survivable Remote server is dropped.

G250 interworking

When calls are made on the gateway while it is controlled by Standard Local Survivability (SLS), the G250, G350, G430 and G450 behave as any Survivable Remote server might behave. The SLS, using its administration and dial analysis plan, can establish local calls from:

- Local station to local station (analog or registered IP)
- Local station to local analog two-way CO trunks

While operating in SLS mode, the G250 attempts to re-register with the primary controller on its MGC list. As soon as the gateway is able to re-register with the primary controller, it un-registers with SLS, and re-registers with the primary controller. In terms of re-registration with the primary controller, the Auto Fallback to Primary feature would therefore work in a similar way with the G250 SLS as it does with the Survivable Remote servers in the G350 or G700.

Note:

The connection preserving aspects of this feature will not be available on the G250 for this release.

G350 interworking

The G350 firmware loads use the Object Identifier (OID) that has the longer Non-Standard Data format in the registration message. This format is only backward compatible to Communication Manager 2.0 loads. Older loads respond with a protocol error as the denial cause for the rejection of the new registration message. Given that the G350 was only introduced in the Communication Manager 2.0 timeframe, it is not backwards compatible with previous Communication Manager releases.

In a startup scenario, there is an exchange of version information between Communication Manager and the gateway. If the Communication Manager load is pre-Communication Manager 3.0, then the auto-fallback mechanism remains disabled for the gateway. Any subsequent registration with a primary controller (from the MGC list) that is running release Communication Manager 3.0 results in the auto fall-back feature being enabled for the gateway.

The only time when the gateway can send a registration message to an older primary call controller is in the rare case when the primary controller has been downgraded while the gateway has been receiving service from an Survivable Remote server. In this case, the gateway receives a protocol error that can be used to send a registration message consistent with Communication Manager 2.0. Downgrading to earlier than Communication Manager 2.0 with a G350 would result in the G350 not being able to register at all.

G700 interworking

The G700 Branch Gateway still uses the same OID as when it was originally deployed. The OID available for the G350 was not ported to the G700. The auto fallback to primary feature requires that all G700s, running the Communication Manager compliant firmware load, use the OID format. The NSD (Non-Standard Data) expansion with the OID is used to carry the context count.

If the gateway receives any of the following errors in response to a registration message, then the gateway sends the original OID registration message prior to the expansion of the NSD.

- 284 - NSD OID invalid
- 283 - NSD OID wrong length
- 345 - NSD Wrong Length - for Communication Manager 1.3 and earlier systems

Though not directly necessary for this feature, the gateway responds to any of the aforementioned protocol errors by attempting to register with the lowest common denominator registration message. The new gateways are backward compatible with even older releases. This modification only applies to the G700.

Older gateway loads

The auto-fallback feature on the server is passive in nature; therefore, an older gateway load trying to register with the current Communication Manager load registers with priority, since the value of the Service-State is that of a gateway without service. Any defined rules for the gateway are ignored, given that an older gateway firmware release tries to register only when it no longer has service from another server; therefore, the administration of rules for old gateway firmware loads are irrelevant.

Adding Recovery Rule to Gateway screen

Procedure

1. Type **`change media-gatewayn`** and press `Enter`.
   The system displays the Gateway screen.
2. In the **Recovery Rule** field, specify the required value.

This field has the following attributes:

- Acceptable values for the field are none, 1 - 50, or 1 - 250, where
  - 50 is the maximum number of supported gateways on an S8300D Server, and
  - 250 is the maximum number of supported gateways on a stand alone server.
- Default is none, which indicates that no automatic fallback registrations will be accepted.
- The value of 1 - 50, or 1 - 250 applies a specific recovery rule to that numbered gateway.

Note:

A single recovery rule number can be applied to all gateways, or each gateway can have its own recovery rule number, or any combination in between.

Result

By associating the recovery rule to the Gateway screen, an administrator can use the **`list media-gateway`** command to see which gateways have the same recovery rules. All the administration parameters for the gateways are consolidated on a single screen. The actual logic of the recovery rule is separate, but an administrator can start from the Gateway screen and proceed to find the recovery rule.

Note:

These changes apply to the **`display media-gateway`** command, as well.

Note:

For more detailed descriptions of the entries and values fields on this screen, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 03-300431, at http://support.avaya.com.

System Media Parameters Gateway Automatic Recovery Rule screens

Definition of recovery rules occurs on the System Parameters Media Gateway Automatic Recovery Rule screens (**`change system-parameters mg-recovery-rule <n>`**. This screen is contained within the 'system-parameters' area of administration screens. The maximum number of screens that can be administered correspond to the maximum number of gateways supported by the server in question, and are:

- Up to 50 for the S8300D Server
- Up to 250 for the standalone Servers

Field description for System Parameters Media Gateway Automatic Recovery Rule screens

Name	Description
Recovery Rule Number	The number of the recovery rule: • Up to 50 for the S8300D Server • Up to 250 for the standalone servers
Rule Name	Optional text name for the rule, to aid in associating rules with gateways.
Migrate H.248 MG to primary	One of four administrable options. The four administrable options are: • **immediately** — which means that the first gateway registration that comes from the gateway is honored, regardless of context count or time of day. The Warning is visible when a user selects this option. This option is the default for all rules. • **0-active calls** — which means that the first gateway registration reporting “0 active calls” is honored. • **Time-day-window** — means that a valid registration message received during any part of this interval is honored. **Note:** Time of day is local to the gateway. There are no constraints on the number of active calls. The time scale provided for each day of the week goes from 00-23 hundred hours (military time). The user must specify an ‘x’ or ‘X’ for each hour where they want to permit the return migration. If they do not want to permit a given hour, then they leave it blank. This method gets around overlapping time issues between days of the week. Users can specify as many intervals they want. • **Time-window-OR-0-active-calls** — means that a valid registration is accepted *anytime*, when a 0 active call count is reported OR if a valid registration with *any*

Name	Description
	call count is received during the specified time/day intervals. **Note:** Time of day is local to the gateway. The time scale provided for each day of the week goes from 00-23 hundred hours (military time). The user must specify an 'x' or 'X' for each hour where they want to permit the return migration. If they do not want to permit a given hour then they leave it blank. This method gets around overlapping time issues between days of the week. Users can specify as many intervals they want.
Minimum time of network stability	Administrable time interval for stability in the H.248 link before auto-fallback can happen. Between 3-15 minutes(Default is 3 minutes).

Recovery rules applied across all gateways

For administrators to see how the recovery rules are applied across all gateways, the Media Gateway Report screen (**`list media-gateway`** command) identifies the recovery rule for each gateway in the network.

```
list media-gateway                                          Page 1 of 1
                          MEDIA GATEWAY REPORT

Num  Name                 Serial No/       IP Address/     Type  NetRgn/   Reg?
                          FW Ver/HW Vint   Cntrl IP Addr         RecRule

1    GW#1 Boxster Lab     01DR11131345     135.8  .77 .62  g700   1        n
                          unavailable                              none

2    MG2 Boxster MV Lab   02DR06750093                      g700   1        n
                          unavailable                              10

3    MG3 Boxster MV Lab   01DR10245104     135.8  .77 .68  g700   1        n
                          unavailable                              none
```

Figure 20: list mg-recovery screen

In this example, gateways #1 and #3 are administered such that no registration request would be accepted by the primary controller when the gateway is active on an Survivable Remote

server. Gateway #2, on the other hand, is administered with Recovery Rule #10. The SAT command:

```
display system-parameters mg-recovery-rule10
```

would show the details of that specific recovery rule.

Administrable IPSI Socket Sanity Timeout

The IPSI Socket Sanity Timeout provides a link-bounce type of interval between Communication Manager and the IPSI to provide resiliency during short network outages. During normal operations, Communication Manager determines the health of a connection to an IPSI by monitoring a heartbeat sent by the IPSI every second. If a heartbeat is missed and Communication Manager does not receive any other data from the IPSI, an IPSI sanity failure occurs. The number of IPSI sanity failures are counted and compared to the value (three to 15 seconds) set by an administrator for the IPSI Socket Sanity Timeout. The administered value of the IPSI Socket Sanity Timeout is the amount of time Communication Manager waits for communication to the IPSI to be restored before a recovery action is initiated. If the value for the IPSI Socket Sanity Timeout is properly engineered, the IPSI is less prone to warm starts and more resilient to short network outages.

If the value of the IPSI Socket Sanity Timeout is greater than three and if there are more than three sanity failures, the port network (PN) is placed in a suspended state. An event is logged recording the transition of the PN from an available state to a suspended state. In a suspended state all messages sent from call processing to the PN and all messages sent from the PN to call processing are delayed until communication resumes. The PN will not go into a suspended state if the value for the IPSI Socket Sanity Timeout is equal to three or if the sanity failures is less than three.

If communication is restored between the server and the IPSI before the value set for the IPSI Sanity Timeout elapses, no action is taken and call processing resumes. If the timer expires before communication resumes, the socket between the server and the IPSI is torn down and Communication Manager attempts to re-connect to the IPSI. It the attempts to reconnect are successful, the PN resets. The type of reset is dependent on the length of the outage. If communication is restored within one minute a WARM restart is performed, after one minute a COLD restart is performed.

For customers upgrading to the latest release of Communication Manager with a value set by Avaya Services other than the three second default, the value set by Avaya Services is carried over during the upgrade.

Note:

The value administered for the IPSI Socket Sanity Timeout has no impact on the Survivable Core server no service timer.

The IPSI Socket Sanity Timeout is administered on page one of the **system-parameters ipserver-interface** form in the **IPSI Socket Sanity Timeout** field. The range for this field is three to 15 seconds with the default set at three seconds.

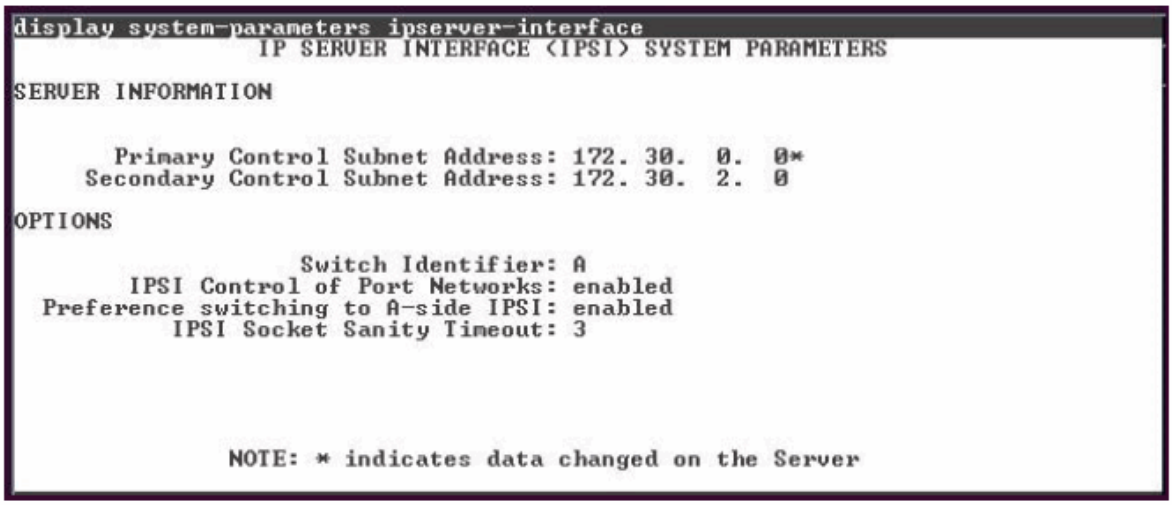


Figure 21: system-parameters ipserver-interface

Survivable Core Servers

The Survivable Core Servers feature provides survivability to port networks by placing backup servers in various locations in the customer's network. The backup servers supply service to port networks in the case where the main server or connectivity to the main Communication Manager server(s) is lost. Survivable Core servers offer full Communication Manager functionality when in survivable mode, provided sufficient connectivity exists to other Avaya components (for example, endpoints, gateways, and messaging servers).

When designing a network to support survivable core servers, consider the following:

- Survivable core servers can only control port networks that they can reach over an IP-connected network.

  That is, Survivable Core servers connected on an enterprise's public IP network will not be able to control port networks connected to control network A or B, unless:

  - Control networks A or B are exposed to the public IP network through control network on the Customer's LAN (CNOCL).

- Multiple Survivable Core servers can be deployed in a network. In the case above, an enterprise could deploy one or more Survivable Core servers on the public network, and an additional server on control networks A and B to backup port networks attached to the respective networks.

However, when port networks register with different Survivable Core servers, system fragmentation can occur. In that case, you should take care to establish adequate routing patterns at a particular location to be able to place calls where needed.

- Survivable Core servers register to the main server(s) through a C-LAN. Each Survivable Core server must be able to communicate with a C-LAN to download translations from the main server. The file synchronization process uses the following ports:
  - UDP/1719 – Survivable Core server registers with the main server
  - TCP/21873 – Main server sends translations to the Survivable Remote server(s) (pre-Release 3.0)
  - TCP/21874 – Main server sends translations to the Survivable Core server (Release 3.0 and above; also for Survivable Remote server translations)

The gateway cannot distinguish between registration through a C-LAN or registration to an S8300D directly. When a gateway completes a successful registration through an IP address defined as a primary call controller address, if that address is a C-LAN, the gateway not necessarily be registered with the true primary call controller. The port network that houses the C-LAN be under control of an Survivable Core server, but the gateway will not know that it is registered with an Survivable Core server.

When the traditional port network migrates back to the primary call controller, then the gateway loses its H.248 link, and the Link Loss Recovery algorithm engages, and that should be sufficient. The Auto Fallback to Primary feature only engages if the gateway drops the connection and registers with an Survivable Remote server. The Survivable Core server migration should only occur if the port network is reasonably certain to return to the primary call controller, so the gateway would simply return to the same C-LAN interface. Now, when the gateway returns to the same C-LAN interface, the Link Loss Recovery feature performs a context audit with the primary controller and learns that the primary call controller is not aware of the gateway. The controller in this case issues a warm start request to the gateway, or potentially different behavior if connection preservation is active at the same time. The auto-fallback feature is not affected by Survivable Core server.

For more information on Survivable Core server, see *Avaya Aura® Communication Manager Survivable Options, 03-603633*.

Improved Port Network Recovery from Control Network Outages

When the network fails, IP-connected port networks experience disproportionately long outages from short network disruptions. The improved port network recovery feature now provides customers using IP connected Port Networks with less downtime in the face of IP network failures.

The feature lessens the impact of network failures by:

- Improving TCP recovery times that increase the IPSI-PCD socket bounce coverage time from the current 6-8 seconds range for the actual network outage to something closer to 10 seconds. Results vary based on traffic rates.
- Modifying the PKTINT recovery action after a network outage to entail a warm interrupt rather than a **PKTINT application reset** (hardware interrupt)). This prevents H.323 IP telephones from having to re-register and/or have their sockets regenerated. This minimizes recovery time from network outages in the range of 15-60 seconds.

This feature also monitors the IPSI-PCD socket and helps in identifying and troubleshooting network related problems.

The IPSI-PCD socket bounce is developed by improving TCP recovery time that covers typical network outages, up to 10-11 seconds range. In this scenario, uplink and downlink messages are buffered, and operations very quickly return to normal after a network failure.To improve recovery time for longer outages, up to the 60 seconds range, the feature introduces the use of a PKTINT warm interrupt rather than a reset. This results in less drastic action being taken to recover links and H.323 IP telephones.

During the network outage, only stable calls already in progress have their bearer connections preserved. A call for which the talk path between the parties in the call has been established is considered stable. Call control is unavailable during the network outage, and this means that any call in a changing state is most likely not preserved.

Some examples are:

- Calls with dial tone
- Calls in dialing stage
- Calls in ringing stage
- Calls transitioning to/from announcements
- Calls transitioning to/from music-on-hold
- Calls on hold
- Calls in ACD queues
- Calls in vector processing

Further, no change in the state of a preserved call is possible. So, features such as conference or transfer are unavailable on the preserved calls. Button pushes are not recognized. Invocation of a feature by the user is given denial treatment. In a conference call, if a party in the call drops, the entire call is dropped.

The following are additional improvements:

- Improve TCP Recovery Time
- Increase IPSI Local Buffering to prevent data loss
- Reduce escalation impact between 15 and 60 seconds by using warm interrupt of PKTINT instead of **PKTINT application reset** (hardware interrupt)

- Reduce escalation impact between 60 and 90 seconds by extending PN cold reset action from 60 seconds to 90 seconds
- Reduce Survivable Core server **No Service Timer** minimum value from 3 minutes to 2 minutes to reduce local customer outage in case of prolonged network outage
- List measurements for the PCD-PKTINT socket for improved troubleshooting

With the introduction of a warm interrupt of the PKTINT instead of reset in the 15-60 seconds range, and the optional extension of the PN cold reset from 60 to 120 seconds.

Port Network Recovery Rules screen

```
change system-parameters port-networks                          Page 2 of 2

                    PORT NETWORK RECOVERY RULES


 FAILOVER PARAMETERS                      FALLBACK PARAMETERS

 No Service Time Out Interval (min): 5          Auto Return: no

    PN Cold Reset Delay Timer (sec): 60
```

Figure 22: PN Cold Reset Delay Timer

No Service Time Out Interval

Field description

Name	Description
2 - 15	No Service Time Out Interval in minutes

PN Cold Reset Delay Timer (sec)

Field description

Name	Description
60 -120 secs	PN Cold Reset Delay Timer in seconds. The default is 60 seconds

Survivability

Reducing the minimum Survivable Core server No Service Time Out Interval from 3 to 2 minutes improves customer overall availability.

Appendix A: PCN and PSN notifications

PCN and PSN notifications

Avaya issues a product-change notice (PCN) in case of any software update. For example, a PCN must accompany a service pack or a patch that needs to be applied universally. Avaya issues product-support notice (PSN) when there is no patch, service pack, or release fix, but the business unit or services need to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a workaround for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.

   Note:

   If the Avaya Support website displays the login page, enter your SSO login credentials.

2. On the top of the page, click **DOCUMENTS**.
3. On the Documents page, in the **Enter Your Product Here** field, enter the name of the product.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. Select the appropriate filters as per your search requirement. For example, if you select Product Support Notices, the system displays only PSNs in the documents list.

Note:

You can apply multiple filters to search for the required documents.

Signing up for PCNs and PSNs

About this task

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new services packs are available. The Avaya E-Notifications process manages this proactive notification system.

To sign up for notifications:

Procedure

1. Go to the Avaya Support Web Tips and Troubleshooting: eNotifications Management page at https://support.avaya.com/ext/index?page=content&id=PRCS100274#.
2. Set up e-notifications.

   For detailed information, see the **How to set up your E-Notifications** procedure.

Index

Numerics

1600-series IP Telephones 104
22621 42
  H2 42
    Duplicated server (IP-connect with single control 42
4600-series IP phone, configuration files 104
4600-series IP Telephones 103
9600-series IP Telephones 104

A

administration 65, 85, 86, 106
  Fax over IP .....
  H.323 Trunk 85
  H.323 Trunks 86
  IP telephones 106
  Modem over IP .....
  TTY over IP .....
  UDS1 circuit pack 65
auto fallback to primary 34
Avaya courses 17

B

bandwidth limitation 168
Best Service Routing (BSR) 91

C

C-LAN 29, 68, 69
  circuit pack TN799DP 68
  installation 69
Call Admission Control (CAC) 168
circuit packs 29
  control LAN (C-LAN) interface 29
CNOCL 59
connecting switches 25
Connection Preservation 33
Control Network on Customer LAN 59
converged networks 63
create 84
  SIP trunk signaling group 84

D

default gateway 71
default node 71
Duplicated bearer 50
Duplicated server 46, 48
  duplicated control 46, 48
  IP-PNC 48
Duplicated server IP-PNC 46
duplicated TN-2602AP circuit packs 41
duplicated TN2602AP circuit packs 90

E

echo cancellation 145–147
  plans (TN464GP/TN2464BP circuit packs) 147
  plans (TN464HP/TN2464CP circuit packs) 146
echo path delay 145
ELS 34
encryption, media 177
Enhanced Local Survivability (ELS) 34
Enterprise Survivable Servers (ESS) 35

F

Fax over IP 126, 129, 153
  administration overview 129
  overview 126
  Super G3 fax machine 153
Fax pass through 134, 136, 137
  bandwidths 136
  considerations for configuration 134
  encryption 137
Fax relay 134, 136, 137
  bandwidths 136
  considerations for configuration 134
  encryption 137

G

G250 Media Gateway 35, 190
G700/G350 Media Gateways 29, 190, 191
gateway 71
  default 71

H

H.248 auto fallback to primary 34, 187
H.248 link recovery 34

H.323 clear channel over IP 126
H.323 link recovery 34
H.323 Trunk 85, 86
administration 85, 86
hardware interface 29

I

iClarity 101
IGAR 27
installation, C-LAN 69
Inter-Gateway Alternate Routing 27
interworking 190, 191
G250 190
G350 190
G700 191
IP codec sets, administering 153
IP interface 90
IP interfaces 89
IP network regions 156
IP Softphone 71, 98
administration 98
Alternate Gatekeeper 71
IP telephone 102, 106
administration 106
IPSI socket sanity timeout 195

J

jitter 29

L

legal notice 2, 5
link recovery 34
load balanced TN2602AP circuit packs 89
LSP 34

M

media encryption 137, 177, 178
FAX, modem, and TTY 137
SRTP 137
support by 178
Mixed PNC 51
mixed reliability with IP-PNC example 51
MM710 T1/E1 Media Module 65
MM760 VoIP Media Module 29
Modem over IP 126, 129
administration overview 129
overview 126
Modem pass through 129, 134, 136, 137
bandwidths 136
considerations for configuration 134
description 129
encryption 137
rates 129
Modem relay 129, 134, 136, 137
bandwidths 136
considerations for configuration 134
description 129
encryption 137
rates 129

N

NAT 117
network 21
converged 21
dedicated 21
IP 21
nondedicated 21
Network Address Translation 117–119
NAPT 118
NAT and H.323 issues 118
Nat Shuffling feature 119
types of NAT 118
network recovery 184
Network regions 22
network regions, IP 156
node 71
default 71
node names, assigning 88

O

overview 63
converged networks 63

P

PCN 201
PCN notification 201
PCNs 201
Per Hop Behaviors (PHBs) 150
port address translation (PAT) 118
port network connectivity 38, 42, 46, 48, 51
Duplex IP-PNC 42
Duplicated server 46, 48
IP-PNC 46, 48
mixed reliability with IP-PNC example 51

S8510 38
IP-PNC 38
PSN 201
PSN notification 201
PSNs 201

Q

QoS 29
Quality of Service (QoS) 29

R

Rapid Spanning Tree 26

S

S8510 38
IP-PNC 38
Session Initiation Protocol (SIP) 83
shuffled connections 149
signaling group 92, 96
signing up 202
PCNs and PSNs 202
SIP trunks 83
SLS 35
spanning tree protocol (STP) 26
SRTP 140
SRTP media encryption 137, 138
for FAX, modem and TTY 137
Standard Local survivability (SLS) 35
STP 26
Super G3 fax machine 153
support 19
contact 19
survivability 33, 184
Survivable Core servers 35
Survivable Remote servers 34

T

T.38 128
T.38 fax 126, 134, 136, 137
bandwidths 136, 137
considerations for configuration 134
overview 126
telephone, IP 102
TN2302AP 72
TN2312BP (IPSI) 29, 77
TN2602AP circuit pack 89, 90
administer for duplication 90
administer for load balancing 89
TN2602AP features 76
TN2602AP IP Media Resource 320 ..... 29, 73, 89, 90
TN799 (C-LAN) 29, 71
Alternate Gatekeeper 29, 71
TN802B MAPD IP Interface Assembly 29
training 17
trunk group 95
trunks 83, 85
H.323 85
SIP 83
TTY over IP 126, 129
administration overview 129
overview 126
TTY pass through 129, 134, 136, 137
bandwidths 136
considerations for configuration 134
description 129
encryption 137
rates 129
TTY relay 129, 134, 136, 137
bandwidths 136
considerations for configuration 134
description 129
encryption 137
rates 129

U

UDS1 circuit pack, administration 65
Universal DS1 (UDS1) circuit pack 65
User Datagram Protocol (UDP) 177, 196

V

video signaling 140
videos 19
Virtual Local Area Networks (VLANs) 152
Voice Activity Detection (VAD) 146